NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A PROPOSAL TO CONDUCT GOVERNMENT CONTRACTING ON THE INTERNET

by

Joseph F. Dunn

June, 1998

Thesis Advisor: Mark M. Stone
Associate Advisor: William J. Haga

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 1998	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE
A PROPOSAL TO CONDUCT GOVERNMENT CONTRACTING ON THE INTERNET

5. FUNDING NUMBERS

6. AUTHOR(S)
Joseph F. Dunn

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The primary purpose of this thesis is to examine the possibility of conducting Government Agency contracting on the Internet. The author proposes that the Internet is a suitable medium on which to process and conduct all aspects of Government contracting. The thesis examines the current legal ramifications surrounding contract formation across the open architecture of the Internet. The thesis then examines the latest cryptological schemes for both encryption and decryption and the logistical challenge of passing keys between participants. The thesis discusses current Federal agencies and current Federal policies regarding encryption and its suitability for Government contracting. The thesis then examines the latest effort among State legislatures and commercial legal ramifications for conducting a contracting effort on the Internet.

14. SUBJECT TERMS
Internet, Cryptology, Public Key Encryption, Rules of Evidence, Digital Signatures, Uniform Commercial Code, Public Key Infrastructure, Authentication, Attribution

15. NUMBER OF PAGES
180

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

A PROPOSAL TO CONDUCT GOVERNMENT CONTRACTING ON THE INTERNET

Joseph F. Dunn
Lieutenant Commander, United States Navy
B.A., University of Denver, 1984

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 1998

Author: _____
Joseph F. Dunn

Approved by: _____
Mark W. Stone, Thesis Advisor

_____
William J. Haga, Associate Advisor

_____
Reuben Harris, Chairman
Department of Systems Management

ABSTRACT

The primary purpose of this thesis is to examine the legal ramifications of conducting Government Agency contracting on the Internet. The author proposes that the Internet is a suitable medium on which to process and conduct all aspects of Government contracting. The thesis examines the current legal issues surrounding contract formation across the open architecture of the Internet. The thesis then examines the latest cryptological schemes for both encryption and decryption and the logistical challenge of passing keys between participants. The thesis discusses current Federal agencies and current Federal policies regarding encryption and its suitability for Government contracting. The thesis also examines the latest efforts among State legislatures and commercial legal ramifications for contracting on the Internet.

TABLE OF CONTENTS

I. INTRODUCTION

A. BACKGROUND

This paper proposes the Internet as an alternative method for contracting electronically in support of electronic commerce. This thesis demonstrates that, there are hurdles to contracting on the Internet. There are legal concerns about formation, signature, and the admissibility of electronic records. There are concerns about security. Numerous Federal agencies and regulations must be satisfied. There is also the interface between Government and commercial contracting procedures that must be addressed. This thesis shows that although there is risk with contracting on the Internet, the risk is no greater than paper systems currently in place. Careful planning and prudent implementation procedures minimize whatever risk is involved with developing electronic contracting on the Internet.

One of the recommendations of the National Performance Review is to increase the use of electronic commerce in Government. By the year 2000, the Federal Government plans to use computers to conduct 75 percent of all practicable transactions. [Ref. 66;p 35-49]

"This activity can occur in 'open systems' such as on the Internet through e-mail and World Wide Web and in more 'closed' systems such as those offered by EDI service providers" [Ref. 33].

To reach that transaction level, the Federal Acquisition Streamlining Act (FASA) of 1994 requires the Government to implement a Government-wide system for electronic commerce--the Federal Acquisition Computer Network (FACNET). [Ref. 66;p 35-49]

FACNET is a closed system. Contractors register with third party Value Added Networks (VANs), VANs register with the Government. VANs monitor access to the system. Regulated access makes the system more secure.

Problems with FACNET and its implementation make alternative solutions necessary. Some of the problems are:

- the central registry is not complete
- the verification procedures are cumbersome
- the information infrastructure is expensive and process errors have occurred in the past

Although FACNET is barely two years old, the Government Accounting Office (GAO) noted that it already is out of step with newer, faster, and more cost-effective

approaches to Electronic Commerce (EC) such as the Internet. [Ref 66;p 35-49]

An Internet solution requires a rethinking of the way participants conduct their business. One of the chief attributes of the Internet is the ease with which participants can connect to each other. One of the essential elements of Internet contracting is finding just the right level of legal predictability without too much regulation. Echoing that view, Ira Magaziner, senior advisor to the President for electronic commerce policy development, stated;

> Companies interested in developing in this area were concerned over the lack of a predictable, legal environment for conducting business electronically... if a digital signature represents different things for different countries, it is very hard to conduct business electronically. Also, people feared that the Government was going to come in and over-regulate, -tax and-censor the Internet and, as a result, strangle electronic commerce. [Ref. 50]

No one solution to contracting electronically can last. Agreement from the majority of participants on how to contract electronically is years away at best. This thesis considers the current state of affairs in the electronic market place, the evolving character of law and technology,

and mechanisms that allow growth and more robust technology insertion as time passes.

Although change is a constant, several anchoring tenets run throughout this thesis. These principles are illustrated in a Clinton Administration policy paper; "A Framework for Global Electronic Commerce";

- the private sector should lead
- Government should avoid undue restrictions on electronic commerce
- where Governmental involvement is necessary, the aim should support and enforce a predictable, minimalist, consistent and simple legal environment for commerce
- the regulatory frameworks established over the past 60 years for telecommunication, radio and television might not fit the Internet
- electronic commerce on the Internet should be facilitated on a global basis. [Ref. 2]

B. OBJECTIVE

The objective of this paper is to provide the legal and technical underpinnings for a legal and secure system of contracting on the Internet.

FACNET, a closed system, is not operating at the volume it was originally planned for. The Internet is an "open" architecture system of computer interfaces that allows greater connectivity than FACNET. Greater

connectivity allows easier access between parties. Connectivity is a prime attribute of doing business on the Internet. On the Internet, anyone with a modem can connect and perform business transactions with any other modem owner.

This aspect of greater connectivity is the chief problem of contracting on the Internet. Greater connectivity makes it more difficult for participants to verify each other's identities and that makes for an unstable business environment.

The thesis addresses the Internet as a medium for exchanging contracting agreements and interacting in a business transaction. It answers the technical and legal questions surrounding Internet contracting. Finally, the thesis proposes an Interchange agreement structure and a benchmark Internet Public Key Infrastructure (PKI, see Appendix C) solution that allows reasonable measured growth as technologies and legal precedents evolve.

C. RESEARCH QUESTION

The primary research question is: What contract formation and authentication requirements are there to using the Internet for Government contracting.

The following subsidiary research questions are addressed:

A. What are some of the areas of contract formation and rules of evidence that need to be addressed before implementing a system of contracting on the Internet?

B. What security measures exist that could aid security in electronic contract formation on the Internet?

C. What Federal Government agencies are involved with electronic contracting on the Internet and what guidelines are already in place?

D. What is the commercial sector and state legislatures doing about electronic contract formation?

E. How can Federal agencies mitigate risk while implementing electronic contracting?

D. SCOPE OF THESIS

Any subject dealing with the Internet is broad in scope by nature. Contracting is also a broad topic that could deal with individual contracts, contractors, agencies or commodities.

The scope of this thesis is limited to generic contracts for over $100,000 and is limited to contracting only with United States contractors. The thesis does not attempt to prove the underpinnings of cryptology and

cryptosystems other than to cite current expert opinion and current security regulations on the subject. The thesis proposes model interchange agreements and public key infrastructure agreements for contracting on the Internet that an Agency can then shape and mold to meet their specific requirements.

E. METHODOLOGY

The author uses one research method to answer the primary and subsidiary questions. The author conducts a comprehensive review of available literature dealing with contract rules of evidence, available cryptology methods, current Federal security requirements, and State legislative actions.

F. ORGANIZATION OF STUDY

This thesis is organized in the following manner: Chapter I is background and introduction. Chapter II examines the legal fundamentals of contract formation. It also examines how those rules apply to forming a contract electronically. Chapter III examines encryption and how it applies to electronic contracting. Chapters IV and V discuss the current Federal environment concerning pertinent public laws, Agencies involved with creating

security policies and current Government security policy. Chapter VI examines electronic contracting in the public sector using states and the Uniform Commercial Code as a proxy for non-Federal policy. Chapter VII provides an integrative analysis. Chapter VIII provides conclusions derived from the research and recommendations for future interchange agreements and public key infrastructure agreements.

II. ELECTRONIC CONTRACT FORMATION

A. INTRODUCTION

Two precedent conditions of electronic contracting on the Internet require specific attention. One condition is meeting all the usual paper-based requirements that make up a legal basis for the contract itself. The other condition is ensuring that the information and terms and conditions that flow between the parties is what the parties have intended and agreed to in their negotiations. This second condition is, for the purpose of this thesis, a need for a secure, a bilateral electronic relationship.

The two conditions are linked. The legal basis for a contract requires competent parties and certainty of terms among other issues. These requirements do not change when contracting electronically on the Internet. In the paper-based system, secure communications are manifested in the final, signed contract. Contracting on the Internet requires additional electronic security measures to ensure the identities of the competent parties and to ensure that no terms or conditions were altered while transiting the open architecture of the Internet. This additional layer of

security is discussed here and is covered more completely in Chapter III that deals with security.

This chapter introduces the legal requirements of contracting in a paper-based system. This chapter builds upon that foundation to establish a legal basis for electronic contracting. This chapter introduces many of the basic machinations of evidentiary requirements that participants need to meet in a paper-based contract. The author describes these requirements as they exist and how they can extend to control the electronic environment in a defensible legal environment.

The chapter suggests that a properly authenticated electronic contract meets all the requirements for executing a contract for all legal purposes.

B. PAPER CONTRACTS

A contract exists where an offer is made by one party (the offeror) to another (the offeree) to contract on specified terms. The offeree accepts the offer and gives something of value to the offeror in return, generally a promise to pay the price specified. This something of value is consideration. [Ref. 29;p. 42]

The common law rules of offer and acceptance provide that a contract comes into existence at the time the offeree's acceptance of the offer (rather than a mere acknowledgement of the offer) is received by the offeror [Ref. 29;p.136]. One exception is where the communication of acceptance is by mail (assuming that postal acceptance is valid) in which case the time at which the contract comes into existence is when notice of the offeree's acceptance of the offer is posted by the offeree to the offeror [Ref. 29;p. 167-170]. This concept is the mailbox rule.

The rules also provide that the place a contract is formed is usually the place where notice of acceptance of the offer is received by the offeror or his agent [Ref. 29;p. 132].

There is no general requirement that the offer, acceptance or evidence of consideration should be in writing or take any particular form except as noted in the Statute of Frauds (infra).

Once a contract has come into existence, participants must consider the terms of that contract. The terms of a contract are those set out in the offer accepted by the offeree. The terms should be clear as to the:

- parties to the contract
- subject matter of the contract
- consideration

An offer frequently provides that an additional body of terms form part of the contract unless there is some mention of a merger clause. A merger clause generally provides that all facets of the agreement are incorporated into the written document [Ref. 29;p. 457]. These terms would usually be the standard terms and conditions of one of the parties.

Absent a merger clause, if a party wants to incorporate terms and conditions into the contract, these terms and conditions must be brought to the attention of the offeree and accepted by the offeree prior to or at the time of the contract coming into existence [Ref. 29;p. 458].

This is why terms and conditions appearing on delivery tickets or invoices alone do not form part of a contract to buy or sell goods. At the time of invoicing and delivery, the parties have already agreed to the contract.

However, terms and conditions appearing on the reverse of order forms would form part of the contract. These terms

and conditions can be agreed to by the parties before the contract is formed.

This is the legal foundation of most of the paper-based contracting system in use today. There are over 200 years of case law that further clarify how courts interpret particular aspects of contract formation or execution.

C. EVIDENTIARY REQUIREMENTS

Case law on the evidentiary requirements of paper-based contracts is well established. The general precept is that the original agreement is brought before the court and the litigants argue their case. "That in proving the terms of a writing, where the terms are material, the original writing must be produced unless it is shown to be unavailable for some reason other than the serious fault of the proponent." [Ref. 41]

A party who wants to rely on a document as evidence in Court should produce the original. In the absence of the original, the Court may accept a copy, but it is for the party seeking to rely on it to prove the authenticity of the copy.

Methods for establishing admissibility are the heart of the evidentiary process. Courts want an original

document because paper documents are hard to change without the change being obvious or recognizable. This may not be the case in an electronic environment. Without proper control, parties can change an electronic document without leaving any marks of how the original document read. This is an objection to accepting electronic documents.

> Judges, juries, attorneys and parties cannot make sound judgments regarding the credibility of computerized records by comparing fairly brief and understandable testimony with recognizable documents, as they could with traditional shop books. Unlike ledgers and books of payables, and receivables with individual items, ... computer printouts are not records at all,... Because program changes or data manipulations can be accomplished without leaving any trace and without affecting the day-to-day operation of a computer system, both unintentional error and intentional fraud are difficult to discover behind a perfect-looking printout [Ref. 3].

If a party introduces a document into court that has been stored in digital form, proving the document represents the original thought or agreement could be difficult if there are no safeguards in place to prevent mistake or fraud.

Case law on the enforceability of electronic and other non-traditional methods of contracting is virtually non-existent. "This is not surprising when one considers that EDI, facsimile communications, and E-mail are relatively recent modes of communication [Ref. 11;p. 64]."

The best measure of how electronic documents will be received in court can be formulated only after examining the current evidentiary requirements in place for paper-based contracts.

1. Statute of Frauds

The English parliament, in 1677, drafted an Act for the Prevention of Frauds and Perjuries. That statute listed a series of 'important' contracts that would not be judicially enforced unless a memorandum signed by the party (or the party's agent) to be charged was produced [Ref. 29;p. 82]. Those contracts were as follows:

- Promises of an Executor or Administrator to pay the debts of the decedent's estate out of his or her own funds
- Promises to pay the debts of another
- Promises upon consideration that a marriage take place
- Contracts for the sale of land
- Contracts which are not capable of being fully performed within one year of the time of their making. [Ref. 11;p. 64]

State legislature have adopted comparable legislation, now known as the Statute of Frauds, in just about every one of our states. [Ref. 29;p. 82]

The Statute of Frauds in the United States, in force since the 1950's, still brings protests and criticisms. The drafting committee working on Article 2 of the Uniform Commercial Code (U.C.C) is debating eliminating the Statute of Frauds as part of their upcoming rewrite of the U.C.C. [Ref. 44]

The primary complaint for those seeking to roll back the Statute is that the Statute of Frauds causes more fraud than it prevents. According to this line of reasoning, the statute permits participants to avoid their obligations under an oral contract which actually had been made, simply because the "technical" or "formal" requirement for a signed writing could not be produced.

The original drafters of the U.C.C. kept the Statute of Frauds in place when dealing with the Sale of Goods. They rewrote the Statute; adding provisions designed to overcome the objections that detractors had aimed at the original statute. [Ref. 54; 259-280]

The Statute of Frauds as embodied in the U.C.C requires an enforceable contract to be in writing, which is

signed by the party against whom enforcement is sought. "Writing" is defined by U.C.C. Section 1-201(46) to include "...[P]rinting, typewriting or any other intentional reduction to tangible form."

Signed is defined by U.C.C. Section 1-201(39) as "[A]ny symbol executed or adopted by a party with present intention to authenticate a writing."

There was early difficulty with considering magnetic and electronic phenomena to be a "reduction to tangible form." It is a fair summary that most jurisdictions consider an electronic record to be a "writing" for Statute of Fraud purposes,[Ref. 60] particularly if the electronic record is capable of being printed onto paper.

Similarly, electronic records such as e-mail or fax communications which evidence directly or circumstantially the sender's assent and self-identification, have generally come to be considered "signed writings" for purposes of the Statute of Frauds. [Ref. 64;p. 16.1-39]

The bar to enforceability under the Statute of Frauds has always been subject to many exceptions, and opinion is building in favor of repealing the Statute of Frauds for the sale of goods and other purposes.[Ref. 53] Regardless whether the Statute is repealed or not, the important point

is that it appears unlikely that electronic records will be held unenforceable under the Statute of Frauds.

2. Best Evidence

The "best evidence rule," Federal Rules of Evidence (FRE) 1001(1), generally requires the use of the original of a writing or recording, defined as;

> Letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other forms of data compilation [Ref. 32].

In the case of computer-produced information, FRE 1001(3) defines the original to include printout or other output "readable by sight, shown to reflect the data accurately."[Ref. 3]

The notion that the original is best is difficult to deal with in an electronic environment. The original in an electronic environment is merely a screen representation of the writing stored in random access memory.

The stored copy is therefore, the first of many copies of the original manifestation on the screen. The primary obstacle for contract formation on the Internet is that the electronic media that the contract would be in can be easily altered without proper safeguards.

The Digital Signature Guidelines published by the Information Security Committee Science and Technology Section of the American Bar Association establishes guidelines that make a copy of a digitally signed message as effective, valid and enforceable as the original of the message. [Ref. 24;p. 88]

3. Hearsay

The law of evidence regards all documents as hearsay. Accordingly, courts can admit documents only as one of the exceptions to the hearsay rule. If a computer produced the document, it is necessary to show that the computer was operating properly at all material times and that a person familiar with the use of that computer is able to give evidence to that effect. [Ref. 20;p. 107]

> Information presented in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor. [Ref. 62]

4. Federal Rules of Evidence (FRE)

a) FRE 1001(3)

The original of a writing or recording as the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it.

b) FRE 1003

A duplicate of the original is always admissible to the same extent as the original unless there is a genuine question as to the authenticity of the original or it would be unfair under the circumstances to admit.

c) FRE 1004(1)

If all originals are lost or destroyed (and if the proponent lost or destroyed them, he did not act in bad faith), then courts permit secondary evidence.

d) FRE 1004(2)

Courts permit secondary evidence if the original cannot be obtained through judicial procedures, such as when the original is in the hand of a third party who is beyond the jurisdiction of the court.

e) FRE 1004(3)

Secondary evidence is admissible if the original is in the opponent's hands and he, after notice, does not produce the original.

f) FRE 1004(4)

Secondary evidence is permitted if the writing is not closely related to a controlling issue in the trial.

g) FRE 1005

Certain types of copies may prove the contents of a Government record of filing (including data compilations).

h) FRE 1006

Summaries of voluminous writings or recordings may be admissible if the writings or recordings are available to the opponent

The sum of all the noted FRE exceptions to admitting the original documentation or an electronic copy are to lay a foundation. If an electronic document can be proven to be an accurate representation of the manifestation to be bound, that evidence in an electronic format can be admissible and can be the basis for determining each

party's respective duties and obligations. The evidentiary problem is not whether an electronic document is admissible. Rather, the court must determine if proper security arrangements are in place to satisfy the court that both parties are who they purport to be and that they have a written agreement determining their obligations.

5. Parole Evidence

The parole evidence rule as reflected in U.C.C. 2-202 is unlike hearsay. Hearsay is a rule of evidence that bars some methods of proof to show a fact but permit that fact to be shown some other way.

"The parole evidence rule bars a showing of the fact itself-the fact that the terms of the agreement are other than those in the writing [Ref. 29;p. 449]."

Parties to a contract often reduce to writing part or all of their agreement, following the negotiation phase. "They do this in order to provide trustworthy evidence of the fact and terms of their agreement and to avoid reliance on uncertain memory [Ref. 29;p. 447]."

There are many reasons why oral communications do not produce perfect understanding. "One is that individual words (or phrases) often carry different meanings to

different persons. And, as many words and phrases are strung together over extended periods of time, such as often happens when contracts are being negotiated, the chances for misunderstanding are markedly increased [Ref. 54;p. 259-280]."

a) Additional Terms

Contract disputes usually arise not because there is a flaw in contract law. Contract law is only the framework from which an agreement hangs. Rather, disputes arise as to the interpretation or construction of the contract between the parties. [Ref 29;p. 445]

Parties can attack a finalized written contract in court in two separate ways. One way is to present evidence that the agreement was actually different from or contradictory of the language in the writing.

The other way is to claim that there are agreed terms in addition to the writing; terms which in no way contradict the writing and, indeed, are consistent with it. This, however, causes a problem where the other side insists that the writing contained all of the terms agreed to; that it was a completely integrated written contract.

"Under current Section 2-202, consistent additional terms--i.e., those that do not contradict the written terms of the writing--may be admitted into evidence ...unless the Court finds the writing to have been intended also as a complete and exclusive statement of the terms of the agreement[Ref 54;p. 259-280]."

In a paper-based system, the participants often sign and exchange the final contract. This serves several purposes:

> **Evidence**: A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
> **Ceremony:** The act of signing a document calls to the signer's attention the legal significance of the signer's act and thereby helps prevent inconsiderate engagements.
> **Approval:** In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing or the signer's intention that it has legal effect.
> **Efficiency and logistics:** A signature on written document often imparts a sense of clarity and finality to the transaction and may less the subsequent need to inquire beyond the face of the document. [Ref 24;p.4]

If participants reach agreement on the Internet, they will not have a final, paper-based document with signatures exchanged. Until working relationships are established, participants will need to take greater care with electronic contracts.

b) Business Records Exception

Although there are other avenues, the principal theory for admissibility of business records--both paper and electronic records--is the "business records exception" to the hearsay rule provided by FRE 803(6), and under various similar State statutes, providing:

> A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of the information or the method or circumstances of preparation indicate lack of trustworthiness. The term 'business' as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.[Ref. 32]

6. Admissibility

Precautions regarding admissibility of evidence in court are intended to prevent tampering with documents after signature. Electronic means exist which can give equal certainty.

For example, it is possible to compute the hash value of a document in digital form, and to send that to an agreed third party. If someone amends the document, the

hash value changes. Comparing the original hash value with a subsequent calculation authenticates the document. (Hash values Chapter III).

"These electronic means, however, do not enjoy the years of tradition of more conventional means of authentication. Therefore, there is a greater risk that the document will not be regarded as admissible [Ref. 20;p.331]."

D. A BILATERAL ELECTRONIC RELATIONSHIP

A new relationship runs concurrently with settled, legal, contractual relationships. "EDI trading amounts to a bilateral arrangement between, for example, a customer and a supplier giving rise to two separate legal relationships between them [Ref. 33]."

One relationship is the ordinary due course relationship, which would exist regardless of the mode of communication of trading data. Paper-based issues of contract formation already discussed apply. The new legal relationship arises from the act of passing electronic data between the parties.

It is this second legal relationship that requires careful planning and precaution. Participants have to agree

to a secure means of transacting their business in an inherently unsecure, open architecture Internet system. The legal basis of contracting cannot be abrogated in this process. The system must be secure to ensure that all participants are who they say they are and that all participants have reliable evidence of their intent to be bound by a contract formed electronically.

If the transmission is secure and the proper legal, paper-based requirements of offer, acceptance etc. are met, there should be no bar to forming a contract electronically instead of on paper. The key is being aware of a concurrent flow of responsibilities.

Security systems and methods for securely transmitting data are available and can be put in place to meet the needs of electronic contracting. Specific security aspects of this new relationship are discussed more completely in Chapter III.

E. CONCLUSION

Contract formation principles on the Internet stay the same as in the paper-based system. The key difference is the method of ensuring that the information and terms and conditions that flow between the parties is what the

parties have intended and agreed to in their negotiations. A bilateral electronic relationship accounts for the additional electronic security measures needed to ensure the identities of the competent parties and their terms and conditions have not been altered while being transmitted on the Internet.

A properly authenticated electronic contract meets all the requirements for executing a contract for all legal purposes.

III. ENCRYPTION AND SECURITY

A. INTRODUCTION

The Internet is open and broadly accessible, which makes it a difficult place for secure commerce. To be a viable alternative for commercial transactions, "any Internet-based system must be able to match the dependability and security of the traditional exchange of paper documents through the U.S. Postal System [Ref. 66;p 35-49]."

Without this level of confidence, transactions on the Internet may be limited as participants maintain the safety and security of paper-based contracting. If Internet users do not believe that their communications and data are safe from interception and modification, they are unlikely to use the Internet on a routine basis for commerce.

A concern is how easily someone can manipulate non-secure electronic documents without any telltale signs of changes. Unsecured information packets can go through any number of computers on the way to reassembling at the target computer. Any number of opportunities exists to alter an unsecured document.

Security in an electronic contracting environment must include the following components:

- the prevention of unauthorized disclosure of information
- the prevention of unauthorized modification of information
- the prevention of unauthorized withholding of information or resources [Ref. 13;p. 41]
- verification that the information is real as opposed to unmodified; This is different than "authentication," which is a procedure used in computer systems to verify a user's identity and/or the unaltered state of the message
- verification that the appropriate party owns or controls the access to the information [Ref. 56]

These security concerns are reflected in numerous state electronic contracting legislative efforts and are discussed in Chapter VI. Cryptology and effective cryptosystems are one answer as to how information remains safe on the Internet.

B. CRYPTOGRAPHY AND CRYPTOSYSTEMS

Cryptography is the art of transforming information to ensure its secrecy or authenticity or both usually using algorithms of varying strengths. Cryptanalysis is concerned with breaking or defeating cryptography. A message before

transformation is called plaintext, and after transformation ciphertext. Transforming plaintext into ciphertext is encryption. Transforming ciphertext back to original plaintext is decryption. A cryptosystem is a collection of algorithms. Algorithms have labels, which are keys. [Ref. 4;p. 350-377]

Plaintext cannot be recovered from the ciphertext in a secure cryptosystem without using the decryption key. A strong cryptosystem has a large key space, which means that there are a large number of possible keys. In this way, it is not practical to use a trial and error method of trying a succession of possible keys to decrypt a ciphertext into its source plaintext.

In a symmetric cryptosystem, a single key is both the encryption and the decryption key. The security of the cryptosystem depends on the secrecy of the key rather than the algorithm.

In an asymmetric cryptosystem, separate encryption and decryption keys are used. A strong cryptosystem generates a ciphertext that appears random to standard statistical tests used to correlate a letter or character in the ciphertext to its counterpart in plaintext.

C. BASIC ENCRYPTION

1. Checksums

A checksum is the simplest form of digital fingerprint--a value, calculated from the content of other data that changes if the data upon which it is based changes. "Checksums have been used since the dawn of computing and are still the basis for error checking in some forms of the popular XMODEM file-transfer protocol [Ref. 49;p. 237]."

If the sum of all the numbers exceeds the highest value that a checksum can hold, the checksum equals the remainder that is left over when the total is divided by the checksum's maximum possible value plus 1.

If A, who sent the document, calculated a checksum of X and B gets a checksum of Y, then the data were altered.

The problem with checksums is that although conflicting checksums are proof that a document has been altered, matching checksums do not prove that the data were not altered.

One can reorder numbers in the document and the checksum does not change. One can change individual numbers

in the document and manipulate others so that the checksum comes out the same.

Capacity is another issue. If the checksum is also a 1-byte value, then it cannot hold a number greater than 255. If A uses 8-bit checksums, there is a 1 in 256 chance that two completely random data streams have the same checksums.

Expanding the checksum length to 16 or 32 bits decreases the odds of coincidental matches, but checksums are still too susceptible to error to provide a high degree of confidence in the data they represent. [Ref. 49;p. 237]

2. CRC

Another way to fingerprint a block of data is to compute a cyclic redundancy check (CRC) value for it. Network adapters, disk controllers, and other devices have used CRCs for years to verify that what goes in equals what comes out. Many modern communications programs use them to perform error checking on packets of data transmitted over phone lines.

The CRC technique protects blocks of data called Frames. Using this technique, the transmitter adds an extra

n- bit sequence to every frame called Frame Check Sequence (FCS).

The FCS holds redundant information about the frame that helps the transmitter detect errors in the frame. The technique is popular because it combines three advantages:

- Error detection capabilities
- Little overhead
- Ease of implementation.[Ref. 21]

The CRC algorithm treats all bit streams as binary polynomials or strings of 0s and 1s. Given the original frame, the transmitter generates the FCS for that frame. The FCS is generated so that the resulting frame is exactly devisable by some pre-defined polynomial. This pre-defined polynomial is the devisor or CRC Polynomial.[Ref. 21]

The receiving end uses the same polynomial for the data and compares its result with the result appended to the message by the sender. If they agree, the data have been received successfully. If not, the sender can be notified to resend the block of data.[Ref. 22]

Polynomial division is the basis of the mathematics behind CRCs. Each bit in a chunk of data represents one coefficient in a large polynomial.

Dividing a polynomial whose coefficients are defined in the CRC algorithm into the polynomial generated from a data stream yields a quotient polynomial and a remainder polynomial. The latter forms the basis of a CRC value.

"If just one bit in a large block of data changes, there is a 100 percent chance that the CRC changes, too. Swapping two bytes or adding 1 to one and subtracting 1 from another does not fool a CRC as it does a checksum."

The problem with a CRC value is that it does not stand up very well to intentional attacks. It is relatively easy for someone with access to a computer to generate a completely different file that produces the same CRC value.[Ref. 29;p. 237]

3. Single Key Encryption

Checksums and CRCs are just two of many different ways to check for message integrity. However, what is missing from that equation is security. Someone could change a message in midstream and simple algorithms cannot catch the change. Here is where more robust encryption schemes can provide both security and message verification.

Two broad categories of encryption schemes are single key encryption (SKE) and dual key encryption (DKE). Public key encryption is another name for DKE.

To implement encryption based on SKE technology, procedures are required to determine how keys are issued and controlled.[Ref. 56;p. 19]

a) DES

One form of SKE in use today is Data Encryption Standard (DES). Federal Information Processing Standard (FIPS) Publication 46 specifies DES as a standard. FIPS and its application is explained more fully in Chapter IV.

This algorithm has a 56-bit key and encodes files in 64 bit blocks. DES is considered very secure, with 2^56 or 7.6 X10^16 possible keys.[Ref. 4;p. 361] However, as processors become more powerful, DES becomes easier to compromise, as all these keys can be tested in a few hours on a supercomputer. To date, no one has cracked DES, but many opine that 56 key technology will soon yield a brute force breakthrough.[Ref. 40;p. 22]

Triple DES, which uses 112 bit keys, uses a three-step process to encrypt data more securely than DES. It has been in use since 1979.

b) IDEA

International Data Encryption Algorithm (IDEA) is designed to be more secure than DES against brute force attacks. This system uses a 128-bit key and an eight-stage algorithm to resist cryptanalysis. The 128-bit key doubles the DES 56 bit key.

The 128-bit key is used to generate 16 bit subkeys. It has a 64 bit block arrangement which is further subdivided into 16 bit sub blocks. There are eight rounds of encryption and a final transformation. Each round operates on four subblocks of plaintext and six subkeys, and the final transformation uses four subkeys.

IDEA is patented in Europe but can be used for non-commercial applications without fee in the United States. It is widely used as part of Pretty Good Privacy (PGP).

4. Dual Key Encryption

A DKE, public key or asymmetric cryptosystem uses pairs of public and private keys that complement each other in performing encryption/decryption of a message.

If A wants to send B a private message, A uses the listed public key of B to encrypt a message for privacy.

How A gets the listed key of B is discussed in the Certificate Authority (CA) paragraphs below.

B applies the private key to decipher the encrypted private message. If A wants to digitally sign the message, A's message is authenticated and signed by hashing the message with a one-way hash algorithm, and then encrypting the hash with A's private key. Hashing and digital signatures are discussed in this chapter.

B then applies A's listed public key to verify that the message was signed by A, and that the message was not modified subsequent to A's signature.

As stated before, the use of single key encryption is somewhat impractical because of the need to share keys with many people. DKE alleviates this problem. The concept of DKE cryptography is appealing because it simplifies some of the problems involved in secret key distribution.

When applied to encryption, it allows a person sending a message to send a message that can only be read by the receiver, without having a need for the sender and receiver to agree on any secret key.

There are some problems with DKE as well as alternatives. "In practice, the methods that have been developed for realizing public key encryption are

comparatively slow, and public key cryptography is generally used for encrypting session keys that are then used for a faster traditional single-key encryption method such as the DES [Ref. 38]."

a) SKIPJACK

NSA designed SKIPJACK and it is the encryption algorithm used in the Escrowed Encryption Standard (EES). EES was the standard that brought clipper chip to data security.

SKIPJACK is classified. It uses an 80-bit key and works on 64 bit blocks of data. It uses 32 rounds of processing and can be used in all four operating modes defined by DES.

There has been public testing and no one has been able to break SKIPJACK to date. Some people believe that the National Security Agency (NSA) has trapdoors in the algorithm that would allow the NSA or other agencies the opportunity to decipher the code without the private key. The NSA and other agencies involved in security are discussed in Chapter IV.

b) RSA

Rivest, Shamir, and Adleman (RSA) pioneered this algorithm. The mathematics behind RSA is based on the fact that the product of two relatively prime numbers is simple to calculate, as a multiplication, but cannot be factored to find those two primes without considerable computational time and expense.[Ref. 34;p. 28]

The key pairs from two random very large prime numbers are multiplied together to form the nucleus used to compute the two keys. In order to defeat the process, these prime factors must be calculated. For a 1024 bit key size, this calculation is considered impractical. This algorithm is secure enough for military or national security uses. The problem with RSA is that it is slow for large key and file combinations.

RSA technology is the standard for the Society for Worldwide Interbank Financial Telecommunication banking network. It is in the X.509 international security standard and will become part of the Internet's upcoming Privacy Enhanced Mail standard.[Ref. 42] X.509 Standard is discussed more thoroughly in Chapter IV.

RSA is a public key cryptosystem that provides both encryption and authentication. It provides two features not found in DES:

- a means for exchanging keys without the prior exchange of secret keys and digital signatures
- the ability for any party to be able to send an encrypted message or verify a digital signature message using publicly available keys.

RSA has a patent in the United States. It has become the standard for encrypting financial and other sensitive data transmitted over the Internet. Many companies using the Internet to transact business, including CyberCash, DigiCash, Microsoft and Netscape, have RSA licenses. MasterCard and Visa have agreed to jointly develop a technical standard (SET) using credit cards over the Internet based on RSA's encryption technology.[Ref. 56;p. 19]

In 1994, RSA Data Security's public key encryption technology was chosen to secure transactions and message exchanges over CommerceNet, a network designed to conduct electronic commerce over the Internet. CommerceNet is operated by the CommerceNet Consortium, a non-profit corporation funded by a three year, $6 million grant from the U.S. Government's Technology Reinvestment Project.

"CommerceNet will win over many skeptics who thought electronic commerce wasn't possible over the Internet [Ref. 28]."

RSA currently licenses its encryption algorithms to companies including Netscape Communications, Microsoft, IBM, AT&T, Motorola, Apple Computer and Sun Microsystems. The RSA technology is also at the center of a proposed system for protecting credit card transactions on the Internet which is being developed by Visa International and MasterCard. [Ref. 37]

c) PGP

Pretty Good Protection (PGP) is a non-commercial encryption program designed for use on the Internet. PGP uses public key cryptography to encrypt files and email messages and to authenticate messages against alteration. PGP prompts the user for a secret phrase before encrypting a file. Only a party who knows the phrase can open the file. To send an encrypted email, the message is encrypted with the recipient's public key. The recipient uses his or her private key to decrypt the message. [Ref. 56;p.19]

PGP works on the principle of public key encryption. Every PGP user has two keys, each one a random

string of bits. One is a public key that is distributed to the world; the other is a secret key the user keeps to himself.

Because the keys are unique, PGP has a second benefit: authentication. Even if the message is not encrypted, the recipient can tell it is from the sender alone as long as the sender used PGP to electronically sign it.[Ref. 14;p. E3]

PGP has been widely deployed by both individuals and businesses around the world in numerous application environments. PGP is both a program for encrypting and digitally signing data as well as a format for sending encrypted messages. [Ref. 36]

D. KEY MANAGEMENT

A weakness of any public key cryptography system is the need to reliably bind the identity of a person to that person's key.

If there is no binding, then C, an imposter could list his own public key in a directory as the key of B, the intended recipient, and then intercept and decrypt a private message intended for B. Alternatively, if A wanted to digitally sign a message, C could insert his public key

as A's public key. C would use his own private key to issue authenticated and signed messages in the forged name of A.

One method of ensuring the secure binding of A's public key to the identity of A, and the binding of B's public key to the identity of B, requires the assistance of CA, a trusted third-party who is sometimes referred to as a Certification Authority, or CA.

A and B both present their public keys to the CA and the CA then adds a digitally-signed public key certificate to A's public key, certifying that "This is A's Public Key," and repeats the process with B's public key.

1. Digital Key Certificates

Digital certificates provide an electronic means of proving identity analogous to a driver's license or passport. A digital certificate binds a user's identity to a digital signature and is verified by a trusted third party.

A digital certificate allows A to verify that a public key belongs to B. Thus, a digital certificate attempts to prevent someone from using a phony key and then impersonating someone else.

A digital certificate contains a public key and a user name. More complex digital certificates can include an expiration date, the name of the certification authority that issued the certificate, a serial number and the digital signature of the certificate issuer.

The standard format for digital certificates is the ITU-T X.509 international standard from the International Telecommunication Union in Geneva, Switzerland. The X.509 authentication scheme can use both secret- and public-key cryptography. While the standard does not require a particular algorithm, the specification does recommend using the RSA algorithm. Digital certificates verify a user's identity only, as opposed to allowing them to conduct a particular type of transaction.

2. Certification Authority

A certification authority (CA) is a trusted third-party that certifies the identities of certificate holders and their association with a given key. Once the CA determines that a request is genuine, it creates a certificate.

After certification, for each message, A encrypts the message with its private key, and appends its public key.

A sends the public key with the message without encryption and it is signed and certified by the CA. B can use the public key sent with the message, or look it up independently, using the CA's public key and the certificate.[Ref. 34;p. 28]

Every certificate contains a serial number and expiration date. Additionally, there is a certificate-revocation list (CRL) that works like a "bad card" list for a credit card company.

There are circumstances when certificates may need to be revoked and put on the CRL. If the key specified within the certificate has been compromised or if the user named in the certificate loses authority, the CA can put the certificate on the CRL.

Two CAs can establish a trust relationship and issue certificates to one another. This is called cross certification.

CAs generally publish their identification requirements and standards on their website. Most CAs will work the same way. A can generate a key pair and send the public key to an appropriate CA, with some proof of identity. The CA checks A's identification and verifies that the request really did come from A. The CA then sends

A a certificate attesting to the bond between A and the public key, along with a hierarchy of certificates verifying the CA's public key. A can present this certificate chain to demonstrate the legitimacy of the public key.

For risk management, B can ascertain the appropriate level of confidence to the issued certificates. CA's with lower levels of identification requirements will produce certificates with lower levels of assurance. For major certificates, significant identification is required. It is all a matter of the level of security needed.[Ref. 59]

3. CA Trust Models

Essentially three different types of CA trust models exist today: Central Authority; Hierarchical Authority; and Web of Trust.

The Central Authority model is based on a single certification authority. This approach was used in early versions of Netscape. However, current versions of Netscape Navigator as well as Microsoft Explorer allow for the installation of alternative certification-authority public keys. [Ref. 59]

The Hierarchical Authority model is when one CA uses a digital certificate from another CA. The highest certification authority in the hierarchy is known as the top-level CA. At the very top of the hierarchy is the root public key. That root public key signs the certificates for all top-level certification authorities, which can then sign certificates for lower-level certification authorities.[Ref. 59]

PGP uses the Web of Trust model. It allows anyone with a certificate to act as a CA by signing another certificate. This model is based on the assumption that, if A trusts B and B trusts C, then A can trust C. As for PGP, if A views someone's certificate with C's signature, then A can trust that signature. The Web of Trust model moves the responsibility of trust to the user. [Ref. 59]

4. Hashing function

A hashing function is similar to a checksum, in that a relatively small hash code can be created from a large file which identifies that file.

A one-way hash function takes messages of variable lengths to produce a hash of fixed length. Once the hash is generated, it is impossible to use the hash to "reverse

engineer" the message. Message digest function is another name for a one-way hash function. [Ref. 5;p. 375]

Typically, hash values are at least 128 bits in length. The greater the length, the more difficult it is to reproduce the input or to find another set of input data that produces a matching result.[Ref.49;p. 237] The hash code is an integral part of a digital signature.

5. Digital Signatures

"Authentication, nonrepudiation and integrity checks can be supported with a digital signature."[Ref. 4;p. 373] A digital signature is a data element that cannot be forged and that verifies the identity of the party who wrote or otherwise agreed to the message to which the signature is attached.

Hash algorithms are combined with public-key cryptosystems to produce digital signatures that guarantee the authenticity of a set of input data the same way a written signature verifies the authenticity of a printed document.[Ref. 49;p. 237]

A hash function produces a message digest. The message digest is encrypted with A's private key. This creates the digital signature. The digital signature is appended to

the message and sent to B. B decrypts the digital signature using A's public key in order to recover the message digest.

B hashes the message with the same hash function that A used and compares the result with the message digest decrypted from the digital signature. If they are the same, then the digital signature has been verified as originating with the A.[Ref. 56;p. 19]

Digital signatures are tied to message content so in some ways, digital signatures are more secure than written signatures. Because written signatures are not message-dependent, one signed paper document allows unlimited imitations by a skilled forger. Digital signatures do not suffer from this problem. [Ref. 34;p. 28]

E. CONCLUSION

The Internet is an open system, where the identity of the communicating partners is not easy to define. The communication path is non-physical and may include any number of eavesdropping and active interference possibilities. This makes Internet communication much like postcards in the mail, which anonymous recipients can answer. To be effective, these postcards must be able to

carry messages between specific endpoints in a secure and private way.

The solution is to use encryption and certification.

To encourage using the Internet for commercial transactions, the Clinton Administration is taking steps to alleviate security fears. "The Administration, in partnership with industry, is taking steps to promote the development of a market driven, public key infrastructure that enables trust in encryption and provide the safeguards that users and society needs [Ref. 2]."

DKE provides a means to implement digital signatures. Separation of public and private keys allows users to sign their data with their secret key, allows others to verify their signatures with the public key, but allows the signer to keep their secret key private.

The private key provides the link between the public key and the individual, and remains a valid link if the user properly maintains the secrecy of the private key.

If for some reason a user's secret key for a digital signature scheme is compromised, then the public key may need to be revoked. If it is known when the private key was compromised, then there is no need to invalidate all of the documents that were signed before this date.

A digital signature serves the same purpose as a handwritten signature on a paper document. A digital signature provides:

- verification that the message originated with the party whose signature is attached
- verification that the message has not been altered since the signature was attached
- a means to preclude the "signer" from later disowning or repudiating the message by claiming that the message had been forged or altered after transmission. [Ref. 56;p. 19]

With these security and encryption measures in place, commercial transactions can be made safe from interception or interference. If electronic contracts can be signed and the signer's identity is securely appended to the electronic document, and if there is clear evidence that the contract has not changed terms or conditions during transmission, then there should be minimal questions as to the validity of the contract and its binding nature on both parties.

IV. FEDERAL REQUIREMENTS

A. INTRODUCTION

There are agencies, policy boards and regulatory committees in the Federal Government that have cognizance over computer security, Internet transactions and/or encryption concerns. Electronic contracting requires a coordinated approach from many different agencies and governing bodies before it can be viable.

This chapter discusses the principal agencies, policy boards and regulatory committees that shape policy in these areas. The second half of the chapter discusses the primary legislation and regulation in place at this time that addresses electronic contracting or the background state of electronic information flow among agencies. Additionally, the chapter addresses the current state of Federal security policy.

This chapter is designed to provide a broad background of the participants and the laws or regulations that have the most impact on an Agency attempting to establish an electronic contracting system. This chapter does not address individual Agency's interpretations of law or regulations.

B. AGENCIES

1. NIST

The National Institute of Standards and Technology (NIST) is a division of the Department of Commerce and was known as the National Bureau of Standards (NBS). NIST is chartered with spelling out security guidelines for unclassified information and has no authority in the classified world.[Ref. 10;p. 37]

NIST issues standards and guidelines that it tries to get adopted by computer systems in the U.S. Official standards are published as Federal Information Processing Standards (FIPS) publications. (FIPS see Chapter V).

In 1987 Congress passed the Computer Security Act, which authorized NIST to develop standards for ensuring the security of sensitive but unclassified (SBU, see Chapter V) information in Government computer systems. It encouraged NIST to work with other Government agencies and private industry in evaluating proposed computer security standards.[Ref. 18]

a) DES

IBM developed DES in 1977 upon which NIST accepted DES as a standard for encryption. This form of encryption uses a single key encryption algorithm.

The drawback of DES is key management, which involves ensuring that User A and User B have arranged for possession of the appropriate key for decryption to occur or the secret distribution of the code. Due to these drawbacks, many encryption experts believe that DES is approaching obsolescence.[Ref. 52]

For years, NIST has promised to come up with a public-key standard for the Government, just as it selected the DES as a private-key standard in 1977. A public-key standard would help legitimize and promote the use of encryption by endorsing a technology that is far easier to use than DES.[Ref. 42;p. 1] DES isolated the Government from the commercial sector, international banking and the Internet community, most of which have thrown their support behind RSA.

b) DSA

The Digital Signature Algorithm (DSA) includes signature generation and verification. Generation makes use

of a private key to generate a digital signature. Verification of the signature makes use of a public key that corresponds to the private key used to generate the signature.

NIST designated this standard for all Federal departments and agencies for the protection of unclassified information. This standard must be used in designing and implementing public key-based signature systems operated by Federal departments and agencies.[Ref. 58;p. 36]

c) DSS

NIST adopted the Digital Signature Standard (DSS) as the Federal standard for authenticating electronic documents.

The DSS defines a public key cryptographic system for generating and verifying digital signatures. The DSS is used with the Secure Hash Standard (SHS) FIPS to generate and verify digital signatures. The Secretary of Commerce approved the DSS as Federal Information Processing Standard (FIPS) 186 (See Chapter V).[Ref. 31]

2. NSA

The National Security Agency (NSA), part of the Department of Defense (DoD) handles classified national security issues. [Ref. 10;p. 37]

NSA and its National Computer Security Center (NCSC) have responsibility for the security of systems and telecommunications collectively known as national security systems. The President has designated the Director of NSA as the National Manager for computer security for national security systems.

National security systems are the systems used by the U.S. Government that;

- contain classified information
- involves intelligence activities
- involves cryptologic activities related to national security
- involves command and control of military forces
- involves a weapon or weapon systems
- involves equipment critical to military or intelligence missions. [Ref. 19]

The NSA, through the NCSC, assists Federal departments and agencies with information security in issues related to national security systems. Services include risk

assessment, security planning, operations security, and identification of security measures.

NSA assesses the vulnerabilities of information systems and provides recommendations on Information Systems Security (INFOSEC) countermeasures that an Agency needs to eliminate or reduce these vulnerabilities.

3. DISA

Defense Information Systems Agency (DISA) is responsible for planning, developing and supporting command, control, communications, computers and intelligence (C4I) and information systems that serve the needs of the National Command Authorities (NCA).

The Agency is responsible for providing communications networks, computers, software, databases, applications and other capabilities that meets the information processing and transport needs of DOD users.

It is the central manager of major portions of the Defense Information Infrastructure (DII see chapter V). It provides guidance and support on technical and operational and information systems issues and coordinates DOD planning and policy for the integration of C4I systems and the

insertion of leading edge technologies into the DII.[Ref. 23]

In its role supporting computer security, DISA recently purchased Netscape Communicator and associated server software.

These products are capable of employing either software-based public key certificates and cryptography at medium assurance level, or FORTEZZA high assurance certificates and cryptography to secure web-based information access across a mix of Unix and Windows platforms.

These products will be used as part of an effort to pilot a medium assurance Public Key Infrastructure (PKI, see chapter V) in support of the Defense Travel System.[Ref. 23]

4. OMB

The Office of Management and Budget is an office in the Executive Office of the President.

OMB's predominant mission is to assist the President in overseeing the preparation of the Federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, OMB

evaluates the effectiveness of Agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. OMB ensures that Agency reports, rules, testimony, and proposed legislation are consistent with the President's budget and with Administration policies.

In addition, OMB oversees and coordinates the Administration's procurement, financial management, information, and regulatory policies. In each of these areas, OMB's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public. In its role overseeing information technology, OMB has implemented several major regulatory policies that affect electronic contracting (see below).

5. GAO

The General Accounting Office (GAO) is the investigative arm of Congress. Charged with examining matters relating to the receipt and disbursement of public funds, GAO performs audits and evaluations of Government programs and activities.

Over the years, the Congress has expanded GAO's audit authority, added new responsibilities and duties, and strengthened GAO's ability to perform independently.

Supporting the Congress is GAO's fundamental responsibility. In meeting this objective, GAO performs a variety of services; the most prominent of which are audits and evaluations of Government programs and activities.

Other assignments are initiated pursuant to standing commitments to congressional committees, and law specifically requires some reviews. Finally, some assignments are independently undertaken in accordance with GAO's basic legislative responsibilities.

In support of this mission, GAO has issued decisions that have affirmed the status of electronic contracting.

6. National Computer System Security and Privacy Board (PSSPB)

Congress established the CSSPB as a public advisory board in the Computer Security Act of 1987. The Board is composed of twelve members and a chairperson who are recognized experts in the fields of computer and telecommunications systems security and technology.

The duties of the Board are:

- to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy

- to advise NIST and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems

- to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress. [Ref. 18]

C. LEGISLATION AND OMB CIRCULARS

1. Computer Security Act

In 1987, the U.S. Congress enacted a law reaffirming that NIST was responsible for the security of unclassified, non-military Government computer systems. Under the law, the role of the NSA was limited to providing technical assistance in the civilian security realm. Congress felt that it was inappropriate for a military intelligence Agency to have control over the dissemination of unclassified information.

The specific purposes of the Act was to assign NIST responsibility for developing standards and guidelines for Federal computer systems, including standards and guidelines security and privacy of sensitive information in

Federal computer systems. The Act allows NIST to seek the technical advice and assistance of NSA. [Ref. 18]

The law was enacted after President Reagan issued the National Security Decision Directive (NSDD) 145 in 1984. The Reagan directive gave NSA control over all Government computer systems containing SBU information. A second directive issued by National Security Advisor John Poindexter that extended NSA authority over non-Government computer systems followed this.

The Act established minimum acceptable security practices for systems. The Act specifies several areas that require attention and specific action among the agencies involved.

Section 20(c) requires that NIST use computer system security guidelines developed by NSA to the extent that those guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

The Act replaced Section 11(d) of the Federal Property and Administrative Services Act of 1949 with new language that:

- empowers the Secretary of Commerce, through NIST, to promulgate standards and guidelines pertaining to Federal computer systems, making the standards compulsory

- authorizes a Federal Agency to employ standards that are more stringent than the standards promulgated by the Secretary of Commerce

- provides that the standards may be waived by the Secretary of Commerce if compliance would adversely affect the accomplishment of the mission, or cause a major adverse financial impact on the operator which is not offset by Government-wide savings. [Ref. 18]

2. OMB Circular A-119

OMB A-119 establishes policies to improve the internal management of the Executive Branch. Consistent with the National Technology Transfer and Advancement Act of 1995, the Circular directs agencies to use voluntary consensus standards in lieu of Government-unique standards except where inconsistent with law or otherwise impractical. It provides guidance for agencies participating in voluntary consensus standards bodies.

The Circular was intended to reduce to a minimum the reliance by agencies on Government-unique standards. [Ref. 15] This Circular and its goals are consistent with acquisition streamlining goals that push for commercial

procedures in lieu of Government standards and military specifications.

The Circular applies to all agencies that use standards and participate in voluntary consensus standards activities, except for activities carried out pursuant to treaties. The goals are:

- eliminate the cost to the Government of developing its own standards and decrease the cost of goods procured and the burden of complying with Agency regulation
- provide incentives and opportunities to establish standards that serve national needs
- encourage long-term growth for U.S. enterprises and promote efficiency and economic competition through harmonization of standards
- further the policy of reliance upon the private sector to supply Government needs for goods and services.

The thrust is to make agencies use voluntary consensus standards, both domestic and international, in its regulatory and procurement activities in lieu of Government-unique standards.[Ref. 15]

3. OMB Circular A-130

OMB Circular A-130 mandates that, as a part of protecting computer systems, agencies incorporate computer security in the system acquisition process.

The Computer Security Act of 1987 and this circular mandated that Agencies protect automated information and the resources used to process it.

To accomplish this goal, computer security and Federal information processing (FIP) procurement must be integrated. The integration is accomplished by incorporating computer security into all phases of the procurement cycle: planning, solicitation, source selection, and contract administration and closeout.

NIST has prepared a Sample Statement of Work for Federal Computer Security Services, which provides assistance to agencies that are contracting for computer security services, such as performing a risk analysis.

4. AECA

Until 1992, the U.S. State Department according to the ITAR (International Traffic in Arms Regulations) regulated the export of cryptography. [Ref. 1]

The State Department, both on its own volition and as advised by DoD and NSA, directly regulates the export of cryptography for reasons of national security.

The U.S. Government considers cryptography to be a defense article or a munition. There are some exceptions,

in which the State Department relinquishes jurisdiction in favor of the Bureau of Export Administration (BXA) within the Commerce Department, for certain types of cryptographic products, typically those employing no or weak encryption.

D. CONCLUSION

The principal agencies exert control over what will be the electronic contracting network. Several agencies and several regulatory bodies exert influence in various aspects of electronic contracting. Additionally, there are overarching goals and standards that the bodies are trying to design or adhere to when they conduct their business.

The chapter shows that, while there are agencies in charge and rules assigned, there is both overlapping and conflicting authority as well as policy coverage gaps where no Agency has the lead.

V. STANDARDS

A. INTRODUCTION

Standards have become critical elements in planning for information systems. Different systems and networks must be interconnected for secure, reliable and accurate transmission and processing of the information.

On the other hand, standards are not rigid. There is room for interpretation in any electronic standard. This chapter highlights some of the current standards and overarching network visions in use today.

This chapter covers the primary standards in place at the Federal level for electronic transactions. The focus is on security and current Federal policy.

B. FIPS

The Computer Systems Laboratory (CSL) of NIST develops Federal Information Processing Standards Publications (FIPS PUBS). CSL issues FIPS under the provisions amended by the Computer Security Act of 1987, Executive Order, and Part 6 of Title 15 Code of Federal Regulations.

The goals of the FIPS program are to:

- improve the life-cycle efficiency and effectiveness of Federal information technology resources

- facilitate the competitive and economic procurement of systems, components and services
- improve the portability of data, software, and technical skills across systems
- protect systems and networks against unauthorized access, manipulation, abuse, and protect information from unauthorized modification or disclosure
- reduce waste, errors, and unnecessary duplication in the application and use of systems
- increase the productivity of the Federal workforce.[Ref. 48]

CSL develops standards, guidelines, test methods, technical agreements, management, physical, and administrative standards for the security and privacy of sensitive information in Federal computer systems. These activities support both Government and industry.

CSL participates in the development of national and international industry standards. They promote open systems. The goal is commercial-off-the-shelf products and services that will serve the needs of users everywhere.[Ref. 48]

1. FIPS 46-2

The Data Encryption Standard (DES) specifies an approved cryptographic algorithm as required by FIPS 140-1.

The key is a 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits are used for error detection.

Data that are considered sensitive (see SBU), that have a high value should be protected if they are vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage.

Cryptographic devices and their technical data are subject to Federal Government export controls as specified in Title 22, Code of Federal Regulations, Parts 120 through 128. Exports of cryptographic modules implementing this standard and their technical data must comply with these Federal regulations and be licensed for export by the U.S. Department of State.

Other exports of cryptographic modules implementing this standard and their technical data fall under the licensing authority of the Bureau of Export Administration of the Department of Commerce. The Department of Commerce is responsible for licensing cryptographic devices used for authentication, access control and proprietary software.

2. FIPS 113

This standard specifies a Data Authentication Algorithm (DAA) which may be used to detect unauthorized modifications to data.

The standard is based on DES and is compatible with both the Department of the Treasury's Electronic Funds and Security Transfer Policy and the American National Standards Institute (ANSI) Standard for Financial Institution Message Authentication. [Ref. 17]

3. FIPS 140-1

This establishes the security requirements that are to be satisfied by a cryptographic module implemented within a security system. It provides four increasing levels of security intended to cover a wide range of potential applications and environments.

The security requirements cover basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic compatibility and self-testing. [Ref. 48] (See also DoD 5200.28 below)

4. FIPS 171

This standard adopts ANSI X9.17 and specifies a particular selection of options for the automated distribution of keying material by the Federal Government using the protocols of ANSI X9.17. ANSI X9.17 defines procedures for the manual and automated management of keying materials and uses DES for key management. [Ref. 48]

5. FIPS 180-1

The Secure Hash Algorithm (SHA-1) is for computing a condensed representation of a data file. When a message of any length less than 264 bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can be input to the DSA which generates or verifies the signature for the message.

The SHA-1 is secure because it is impractical to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit results in a different message digest, and the signature fails to verify.

This standard is required for use with DSA as specified in the DSS and whenever a secure hash algorithm is required for Federal applications.[Ref. 48]

6. FIPS 185

The Escrowed Encryption Standard (EES) provides an encryption/decryption algorithm and a Law Enforcement Access Field (LEAF) creation method, which agencies can implement in electronic devices and use to protect Government telecommunications.

The LEAF is used in a key escrow system that provides for decryption of telecommunications when access to the telecommunications is lawfully authorized.[Ref. 48]

The algorithm of EES is Skipjack (chapter III) developed by NSA. The Clipper Chip portion of EES pertains to digital telephony, and projects the use of a hardware-implemented Skipjack algorithm.

EES requires that one of the keys be split in two and held in escrow by two Government custodians. This allows a Government law enforcement Agency to obtain the keys from the escrow custodians, enabling the Government to eavesdrop on the otherwise confidential communications.

7. FIPS 186

This Standard specifies a DSA appropriate for applications requiring a digital signature. The DSA is a pair of large numbers represented as strings of binary digits. Signature generation and verification are through a public key/private key arrangement.

The message digest is input to DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the data.

The receiver verifies the signature by using the sender's public key. The hash function is specified the Secure Hash Standard (SHS), FIPS 180.

This standard must be used in designing and implementing public-key based signature systems which Federal departments and agencies operate or which are operated for them under contract.

DSS is mandatory for use by Federal agencies and their contractors.[Ref. 61;p. 10] However, it seems that NIST-standard cryptography such as the Escrowed Encryption Standard (EES) and DSS are hardly used in Government, and virtually not at all by industry.

C. DOD 5200.28-STD

The NCSC published 36 books known as the Rainbow Series. Each book in the Rainbow Series details a specific aspect of computer security. One of the first is the Orange Book, officially titled the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC).

The Orange Book identifies four security levels, ranging from Division D to Division A. The levels in use currently are D, C1, C2, B1, B2, B3, and A1.

Each level sets a minimum security threshold that a system must meet in the hardware, software, operating system or firmware.

Divisions are segmented into classes. Each rating outlines system requirements based on security policy, accountability, assurance, and documentation, and builds upon the prior rating.

1. Division D

The least secure rating is Division D--minimal protection of a computer network. According to the Orange Book, this division contains only one class. It is reserved for those systems that have been evaluated but that fail to

meet the requirements for a higher evaluation class. Products or systems in this class are not secure.

2. Division C

Level C is discretionary protection where information is provided on a "need-to-know" basis. Division C systems are nominally secure.

a) C1.

A Class C1 rating means user access to files is controlled, although files can be shared. Users must identify and authenticate themselves, and data must be protected from unauthorized users. The trusted computer base (TCB) should protect itself from outside tampering. The C1 rating requires periodic testing of the hardware and software on the system.

b) C2.

The 1987 Computer Security Act requires that all Federal agencies with sensitive but unclassified (SBU) information protect their systems to the C2 level or equivalent [Ref. 18]. C2 systems must limit users' access

to data. Only authorized individuals can assign access rights to individuals or groups of users. The TCB has to create an audit trail and protect against unauthorized access, changes, or destruction of the audit trail. The audit has to monitor the time and date, type, and success or failure of each event. The TCB needs to record:

- user identification and authentication
- which files or programs a user uses
- when and which objects are deleted
- the actions of computer operators, system administrators, and/or system security officers
- 'other security-relevant events'

3. Division B

Division B is Mandatory Protection. This division uses sensitivity labels to determine whether a user can access a particular object.

a) B1.

Class B1 requires an informal statement of the security policy model, data labeling, and mandatory access control. The B1 class establishes security clearances as well. The TCB also checks to make sure that the security clearances of outside parties were granted by an authorized user. Audits at the B1 level must also record an object's security level and track activities based on user identity and/or object security level.

b) B2.

This level requires a formal security policy and proof that the system upholds that policy. The B2 system must include a mechanism to guard against outside or unauthorized interference or tampering. Least privilege is enforced. Least privilege grants the user the most restrictive clearance required to complete the task. Hardware is used to separate objects with differing attributes, and user interfaces to the TCB must be defined and all elements identified. The operator and administrator functions must be separate.

c) B3.

Class B3 is the highest rating in Division B, and the second-highest Federal security level. A B3-rated TCB is highly resistant to penetration and is tamperproof. Code that is not essential to enforcing the security policy is excluded. B3 systems are designed to minimize complexity. The system supports a security administrator and an audit mechanism that signals security-relevant events. B3 is also the first level that addresses system-recovery procedures.

4. Division A

Class A1 signifies the most secure Federal system. A1 systems must cite a formal model of the security policy and include mathematical proof that the model supports the policy. Beyond A1, the Orange Book suggests the possibility of a future class, based on advanced technologies as a means for advancing the standards.

D. DII

The Defense Information Infrastructure (DII) is a planned web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services.

The DII Master Plan provides the baseline description of DII policy, guidance, strategies and initiatives. It is a management tool for identifying DII voids, discrepancies, issues, and opportunities.[Ref. 23]

The DII is akin to the National Information Infrastructure (NII) that is seeking to link all aspects of the Federal Government in a seamless computer web.

E. SBU

Sensitive But Unclassified (SBU) information is information where the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests.

National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government.

Other Government interests are those related to the wide range of Government information or commercial proprietary information provided to the U.S. Government.

"Federal Departments and Agencies shall ensure that telecommunications and automated information systems handling SBU information protects such information to the level of risk and magnitude of loss or harm that could

result from disclosure, loss, misuse, alternation, or destruction [Ref. 47]." Federal contracting information falls into the SBU category and requires special security.

F. X.509

Most public key certificates available today are based on an international standard ITU-T X.509 version 3.

NIST has developed a hybrid architecture specification based on both a hierarchical and a network architecture model in the document, *Public Key Infrastructure (PKI) Technical Specifications: Part C - Concept of Operations.*

This standard defines a certificate structure that includes several optional extensions. The use of X.509 v3 certificates is important because it provides interoperability between PKI components. Provisions in the X.509 standard enable the identification of policies that indicate the strength of mechanisms used.

The rules expressed by certificate policies are reflected in certification practice statements (CPSs) that detail the operational rules and system features of CAs and other PKI components.

By examining a CA's CPS, users can determine whether to obtain certificates from it, based on their security

requirements. Other CAs can also use the CPS to determine if they want to cross-certify with that CA. [Ref. 65]

The ITU-T Recommendation X.509 defines a framework for the provision of authentication services. It describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed by using cryptographic techniques.

X.509 is an ITU Recommendation. Consequently, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use X.509 certificates to implement Secure Socket Layer (SSL) in their Web servers and browsers. But an X.509 Certificate generated by Netscape may not be readable by Microsoft products, and vice versa. [Ref. 65]

G. PKI

Public Key Infrastructure (PKI) provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large networks. Public keys are bound to their owners by public key certificates. These certificates contain information such

as the owner's name and the associated public key and are issued by a reliable Certification Authority (CA).

NIST has produced a Minimum Interoperability Specification of PKI Components [MISPC]. The MISPC was produced in cooperation with industry partners. The MISPC specifies a minimal set of features, transactions, and data formats for the various certificate management components that make up a PKI. The specification addresses certificate generation, renewal, and revocation; certificate validation; signature generation and verification; and other related issues.

NIST is producing a Security Baseline document. The Baseline should help to establish operational practices and provide criteria for evaluating service and equipment offerings.

The U.S. Federal Government Information Technology Services (GITS) board has established a Federal PKI Steering Committee to provide guidance to Federal agencies regarding the establishment of a Federal PKI. [Ref. 30] The Federal PKI Steering Committee sanctions approximately fifty PKI-related pilots throughout the Federal Government.

NIST is coordinating with industry and technical groups developing PKI technology such as the Federal PKI

Steering Committee and its Technical Working Group (TWG), CommerceNet, Internet's PKIX, and the Open Group.

NIST is also developing of a Reference Implementation and the initial implementation of a root Certification Authority (CA) for the Federal PKI.

The initial implementation of a root CA involves the development of a procurement specification for a CA based on the MISPC and the procurement of an operational CA. [Ref. 48]

H. CONCLUSION

There is any number of standards or goals for interoperability of computers at the Federal level. Each attempts to standardize meets the same conundrum, set the standard too rigid and no one will use it. Set the standard too loose, and it is not a standard.

The author predicts that there will never be one universal standard that all participants agree to use. Rather, there will be baselines of interoperability and minimum security levels that participants agree to uphold. The Federal Government is a large player in the setting of standards based simply on the volume of business that Government transacts. Continuing to emphasize commercial

standards prevents Government agencies from developing expensive, proprietary solutions to common commercial concerns.

VI. STATE AND COMMERCIAL STANDARDS

A. INTRODUCTION

This chapter will survey the changes being proposed or already in force at both the state and commercial level.

More than two thirds of state legislatures have either enacted, or are currently considering, legislation addressing issues raised by electronic contract formation. Additionally, the law that governs commercial contracting is being updated to account for changes in the commercial environment.

This activity evidences the importance of the subject, and is an effective barometer for the electronic contracting climate as a whole. There are problems, however.

Multiple authorities are writing statutes and case law is largely unsettled or non-existent. "There is little consensus on how to approach the subject. Moreover, several states have recognized that the subject requires more study before the appropriate legislative solution can be determined [Ref. 55]."

For the most part, at least one state has considered or enacted legislation on some major issues surrounding

electronic contract formation. Since Federal courts may consider state law where no Federal legislation governs, there is a necessity to review state legislation to discern the patterns of legislation that may prevail in case of a dispute.

The Uniform Commercial Code (U.C.C.) has governed commercial transactions since its inception. It had a large impact codifying and standardizing interstate commerce and will have a large impact on electronic contracting. "In the United States, every state Government has adopted the [U.C.C.]. ... [Article 2B is] working to adapt the U.C.C. to cyberspace. ... The administration supports the prompt consideration of these proposals, and the adoption of uniform legislation by all states. *White House Report, Framework for Global Electronic Commerce, (July 1, 1997)* [Ref. 45;p. 3]"

B. UTAH

On March 10, 1995, the State of Utah enacted a Digital Signature Law, based upon a public key cryptosystem supported by a system of certification authorities.

The legislation marks one of the earliest attempts to craft enabling legislation to create an electronic system

for authenticating electronic records. The legislation addresses time stamping as another means to certify and verify the receipt of a document in a legally acceptable and verifiable manner. "The laws by Utah and the state of Washington are considered the most comprehensive and serve as models for other states [Ref. 39]."

The Act addresses concerns about the identity of the sender or recipient of electronic communications and the proof of a signature. It creates a scheme based on public key cryptography, in which digital signatures are certified by a network of Government-licensed certification authorities.

Its purposes are:

- to minimize the incidence of forged digital signatures and enable the reliable authentication of computer-based information
- to enable and foster the verification of digital signatures on computer-based documents
- to facilitate commerce by means of computerized communications.

The Act creates Government-licensed certification authorities containing the name of the subscriber and the subscriber's public key.

In accepting the certificate, the subscriber certifies that each digital signature is valid. The subscriber certifies that no unauthorized person has access to the private key. The subscriber has to exercise reasonable care in retaining control of the private key and keeping it confidential.

Under the Act, a digital signature is as valid a handwritten signature. The statute creates a presumption that a digital signature verified using a public key is attached with the intention of the subscriber to authenticate the message and to be bound by the contents of the message.

The presumption can be refuted by proof that the digital signature cannot be verified by reference to a certificate issued by a licensed certification authority, or that the subscriber lost control of the private key, or by evidence showing a lack of a signature at common law, or by evidence that reliance on the presumption was not commercially reasonable.

"As of this writing, bills have been introduced into the State Legislatures of California and Washington State, closely resembling the Utah Digital Signature Law [Ref. 3]."

C. OTHER STATES

1. Introduction

Other states have also adopted legislation to deal with the coming wave of electronic contracting, filing, and registration that many hope will speed up the wheels of Government while at the same time increase accuracy and decreasing cost.

2. California

Bill 1577 provides the use of a digital signature shall have the same force and effect as the use of a manual signature if it embodies all of the following attributes:

- it is unique to the person using it
- it is capable of verification
- it is under the sole control of the person using it
- it is linked to data in such a manner that if the data are changed, the digital signature is invalidated
- it conforms to regulations adopted by the Secretary of State. [Ref. 8]

3. Indiana

Senate Bill 5a provides that a digital signature on a document received by or filed with the state is effective if:

- it is unique to the person using it
- it is capable of verification
- it is under the sole control of the person using it
- it is linked to data in such a manner that if the data are changed, the digital signature is invalidated
- it conforms to regulations adopted by the State Board of Accounts. [Ref. 55]

4. New Hampshire

Senate Bill 207 provides that an electronic signature shall have the same force and effect as a manual signature if the signature is:

- unique to the person using it
- verifiable
- under the control of the person using it
- linked to the data in such a manner that if the data is changed the signature is invalidated
- conforms to administrative regulations. [Ref. 58]

5. Texas

House Bill 984 establishes the equivalence of written and digital signatures and allows digital signatures to authenticate written electronic communications sent to state agencies.

A person may attach a digital signature to communications with State agencies if a digital signature is:

- unique to the person using it
- capable of independent verification
- under the sole control of the person using it
- transmitted in a manner that will make it infeasible to change the data in the communication or digital signature without invalidating the digital signature. [Ref. 6]

6. Virginia

Senate Bill 153 authorizes the use of electronic signatures. The Act provides that the state and its agencies can use electronic signatures only if such signature is:

- unique to the signer
- capable of verification
- under the signer's sole control, or

- linked to the record in such a manner that it can be determined if the any data contained in the record is was changed subsequent to the electronic signature is invalidated being affixed to the record,

- created by a method appropriately reliable for the purpose for which the digital electronic signature was used.

A judge may consider any other relevant and probative evidence affecting the authenticity and/or validity of the electronic signature. [Ref. 17]

Senate Bill 923 provides for the legal recognition of electronic signatures and authorizes state agencies to use electronic signatures. [Ref. 17]

7. Wisconsin

Assembly Bill 100 permits the Department of Administration to accept electronic signatures concerning state construction contracts, bids and proposals, if the electronic signature embodies these five attributes;

- the digital signature is verified by a certification authority

- the person who is to receive the document consents to the use of the digital signature

- the digital signature was created by a particular person

- the document to which the digital signature is affixed has not been altered since the digital signature was created

- the digital signature conforms to any rules promulgated by the Department.

A digital signature that satisfies all of these factors would have the same force and effect as any other form of signature.[Ref. 58]

8. Kansas

House Bill 2059 provides that a digital signature may be accepted as a substitute for and shall have the same force and effect as any other form of signature. The guidelines are:

- intended by the party person using it to have the force and effect of a signature

- unique to the party person using it

- capable of verification

- under the sole control of the party person using it

- linked to data in such a manner that it is invalidated if the data are changed.[Ref. 5]

9. Florida

Senate Bill 942 authorizes the use of digital and electronic signatures for signing writings electronically

and authorizes the Secretary of State to act as a CA.[Ref. 26]

House Bill 1413 allows notaries public to perform electronic notarizations using a digital signature. In the event a notary's private key is compromised, the notary is required to notify the Secretary in writing and to request the issuing CA to suspend or revoke the certificate.

The Act authorizes the Secretary of State to establish a voluntary licensure program for private CA's and to make rules necessary to implement and enforce the program.[Ref. 58]

10. Minnesota

Senate Bill 173 provides for licensure of CAs, performance audits and investigations, requirements for and obligations of CAs, controls of private keys, suspension, revocation and expiration of certificates, recommended reliance limits and liability, presumptions in adjudication of disputes, and standards for recognition of repositories.[Ref. 43]

Additionally it is designed to:

- facilitate commerce by means of reliable electronic messages

- minimize the incidence of forged digital signatures and fraud in electronic commerce

- implement legally the general import of relevant standards, such as X.509 of the International Telecommunication Union

- establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages. [Ref. 43]

11. Mississippi

House Bill 752 authorizes the Secretary of State to serve as the CA to verify the digital signature of any public entity in Mississippi.

With the bill, digital signatures verified by a licensed certification authority will have the same force and effect as a written signature. [Ref. 58]

12. Oregon

House Bill 3046 authorizes the use of electronic signatures and provides that they have the same force and effect as a written signature. It also authorizes the Government to issue certificates for the purpose of verifying digital signatures and to suspend or revoke certificates. The Department is authorized to register certification authorities to ensure the integrity of digital signatures. [Ref. 58]

13. Washington

Senate Bill 5308 provides that the Secretary of State is a CA, and that certificates issued by the Secretary have the same effect as a certificate issued by a licensed certification authority. It grants the Secretary discretionary authority to adopt rules to govern CA's and repositories. It also addresses suspension and revocation of licenses.[Ref. 27]

14. New Mexico

House Bill 516 provides

- a centralized, public, electronic registry for authenticating electronic documents by a public and private key system
- promotes commerce
- facilitate electronic information and document transactions

An "office of electronic documentation" is established under the Secretary of the State to maintain a register of public keys. The Secretary of State is required to adopt regulations to accomplish the purposes of the act, and may contract with a private, public or quasi-public organization to provide services under the Act.[Ref. 7]

15. Illinois

House Bill 597 applies to communications with financial institutions to give electronic documents and signatures the same force and effect as their manual counterparts.

The Act also amends the Criminal Code to provide that unlawful use of an electronic signature constitutes a forgery punishable as a felony. [Ref. 58]

16. Louisiana

House Bill 294 provides for the admissibility into evidence of promissory notes and certain other records relative to financial institutions that contain signatures created and stored electronically or digitally.

If any such record has a signature electronically or digitally rendered, any printout or other output readable by sight, accurately reflecting the data, will be deemed an original. [Ref. 58]

D. UNIFORM COMMERCIAL CODE

1. Introduction

Article 2 of the Uniform Commercial Code (U.C.C.) governs the sale of goods in the United States. Its

relevance has been enhanced by judicial extension to the licensing of commercial software products as the practical equivalent of a sale.[Ref. 51;p. 10]

The original U.C.C. was written and codified more than half a century ago and accepted by all states except Louisiana. Most state commercial codes were also drafted at about this time. Since then, the whole idea of electronic commercial transactions has arisen.

Although written as a flexible standard, the U.C.C. does not adequately address electronic transactions. The various codes impacting purchasing transactions were drawn before computers had commercial impact.[Ref. 35] That is why the U.C.C. is undergoing a substantial review.

The legal organizations that sponsor the U.C.C. are nearing the end of a major revision and expansion of it. When the revisions end, it will have left only one of the original nine articles in the code untouched and will have added three new ones.[Ref. 12]

2. U.C.C. Committee

The American Law Institute (ALI) and the National Conference of Commissioners on Uniform State Laws (NCCUSL) want to change to accommodate and update the code to

reflect "new legal thinking, new technology, and the transition from an economy based on manufacturing to one built on services and information [Ref. 12]."

Under NCCUSL rules, the National Conference must consider any proposed new Article 2, section by section, no less than twice before deciding to approve it. A majority of states present, each with one vote, must approve the draft and there must be at least twenty approving jurisdictions. Representatives may submit proposed code to the ABA for its consideration.[Ref. 44;p. 4] By design, this is a lengthy process to ensure that the issues addressed are substantive and that recommendations are based on sound legal thinking and can be properly implemented.

3. Article 2B

Article 2B deals with information transactions. It focuses primarily on software, on-line and Internet commerce information and licenses for data, text and similar materials. However, it is also a contract statute. As such, it deals with contractual relationships.

Article 2B provides a framework for contractual relationships among participants. Article 2B attempts to

distribute risk and benefit among the various parties who are conducting their business electronically.[Ref. 45;p. 40]

a) Authentication

The term "authenticate" replaces "signature" or "signed" in 2B. The section expands the traditional concept of signature. The aim of the drafters is to remain technologically neutral. This neutral approach is endorsed by Federal Government reports on electronic commerce.

Encryption and other technologically enabled acts can be used to achieve a signature. The critical factor lies in the intent of party making the authentication.

Statutes in some states give special recognition to digital signatures that rely on a specific encryption technology and a certification or licensing system. The procedures in those statutes qualify as authentication for Article 2B.

Any execution of a symbol with the intent to sign that would be a signature under prior law, is an authentication under Article 2B.

Authentication can have various effects. Absent circumstances indicating a different intent, an authentication: [Ref. 45;p. 32]

- establishes the parties identity
- the acceptance of the record or term
- the acceptance of the contract
- confirms the integrity of the records or terms as of the time of authentication. [Ref. 45;p.75]

b) Authentication Liability

An electronic authentication is attributable to person A if it was the action of A, A's human agent, or A's electronic agent.

Liability arises if B, in accordance with a reasonable attribution procedure for identifying A, in good faith concluded that a message or action was an act of A, A's agent, or A's electronic agent. Attribution is necessary because both parties need to be able to rely on the identity of the participants.

A is liable for losses if the losses occur because A failed to exercise reasonable care; B reasonably relied on the belief that A was the source of an authentication; B's reliance resulted from acts of a third person that obtained

access numbers, codes, computer programs, or the like from a source under the control of the person that failed to exercise reasonable care; and the use of the access numbers, codes, computer programs, or the like created the appearance that it came from A. [Ref. 45;p. 69]

c) Attribution

Attribution may include various approaches, including algorithms, codes, identifying words or numbers, encryption, or other reasonable security device.

A court determines commercial reasonableness of an attribution procedure. To make this determination, the court can look to several factors. One way the court can determine commercial reasonableness is if the process is established by law or regulation. If it is, the court can assume it is commercially reasonable.

Another factor a court can look to determine commercial reasonableness is to review prior course of dealings and the circumstances surrounding the transaction at the time the parties agree to adopt the procedure. [Ref. 45]

d) Electronic Formation

Section 2B-113 states a fundamental principle of electronic contracting. "A record or authentication may not be denied legal effect, validity, or enforceability solely on the ground that it is in electronic form [Ref. 45;p. 65]."

It stems from digital signature and electronic signature law in several states. The mere fact that a message or record is electronic does not alter or reduce its legal impact.

This principle is restricted to the scope of Article 2B. It does not necessarily deal with other legal instruments necessary for electronic commerce. Under Section 2B-103, the subject matter of those other areas is excluded from Article 2B.[Ref. 45;p. 67] However, the Federal Rules of Evidence and numerous court cases on the subject should form the basis for the legal sufficiency to conduct business electronically.

e) Electronic Agency

The draft develops a system where either no human decision is necessary or a human interacts with a computer

for the processing of a legal contract. It relies on an offshoot of the concept of agency.

Electronic agents can form the contract. The specific terms of the contract are determined under Section 2B-209(b). A contract is formed by an electronic agent and an individual if the individual has reason to know that they are dealing with an electronic agent. The example given is if a person telephones in an order and connects to a computer. If the individual takes actions that cause the agent to perform or accept, a contract is formed, regardless of other expressions or actions by the individual to which the electronic agent cannot react.

The last part of the clause is so that a human cannot order something and predicate payment on a new term or condition that the computer is not programmed to understand. This also aligns with the usual notions of terms and conditions in use now. The terms of a contract formed under this paragraph are determined under Section 2B-207 or 2B-208.

f) ***Electronic Mailbox Rule***

An electronic message is effective when received even if no individual is aware of its receipt. If an

electronic message sent by a party evokes an electronic message in response, a contract exists when a response signifying acceptance is received or if the response consists of furnishing the information or access to the information, when it is received, unless the originating message required acceptance in a different manner. [Ref. 45;p. 75]

g) Parole Evidence

Section 2B-301 addresses parole evidence. The basic requirements of parole evidence remain unchanged. If participants sign a contract with a merger clause, the final record cannot be contradicted but it may be explained or supplemented by prior course of dealings and consistent additional terms.[Ref. 45;p. 103]

E. CONCLUSION

The state and the U.C.C. approaches are both concerned with issues of positive identification of the participants. Most of the basic contract formation principles have been left intact with only minor modifications to account for the transmission medium.

The U.C.C. focuses on the intent of the parties. If the parties intend to be bound, they will ordinarily be

held bound. [Ref. 11;p. 4] In general, parties are able to do business with each other on the Internet under the terms and conditions they agree upon. Participants in electronic contracting, through legislative statute and U.C.C. revisions, are developing a framework to achieve predictable and accepted legal principles to support electronic commercial transactions.

State legislatures and the drafters of the U.C.C. are promulgating proposed standards and contracting paradigms to enable participants to predict what effect their agreements might have when evaluated by a court. Many of these efforts are in the nascent stages. Many questions remain concerning how a court will evaluate participants conduct and understandings in case of a dispute. Any Agency initiating an electronic contracting procedure will have to deal with large amounts of uncertainty until case law and precedent flesh out the proposed legal frameworks.

VII. ANALYSIS

A. CONTRACT LAW

The change to an electronic contracting environment from a paper-based system does not necessitate changes in the underlying legal theories and principles. The primary change is in the method of transmission, and not in the rudimentary formation concepts. Legal documents transmitted across the open architecture of the Internet will require certain security safeguards be in place and maintained in order to satisfy formation issues and evidentiary issues.

Cryptological procedures currently exist that can solve the security problems. Rules of evidence already account for introducing electronic evidence. Commercial transactions are already being consummated across the Internet. State legislatures are building a foundation for electronic commerce at the state level. Commercial concerns, as embodied by the U.C.C. are addressing the issues that impact electronic contracting transmission.

In creating a uniform law for electronic contracting, NCCUSL is keeping the elements of contract law and commercial law relatively intact. The primary changes are in the method of delivery or transmission of the final,

agreement and not in the formation of the agreement. This is in accordance with the idea of a bilateral electronic relationship wherein only the method of transmission has changed significantly. That change has necessitated a change in the validation procedures needed to ensure a contract is formed. As long as the goal of the electronic contract does not breach fundamental concepts of contract formation (e.g. competent parties, legal aim) and the messages transmitted are adequately secured, the resulting electronic contract should be binding and legal.

For agencies looking to adopt electronic contracting policies, their focus can be on the transmission aspects and their answers will be mostly in the realm of their information technology (IT) group and not the legal department. Maintaining up-to-date market information about the latest technology and implementation procedures will be a key aspect of any implementation plan. An Agency will best be served with a plan that allows modular updates to processes and procedures to account for the technology enhancements that are sure to come in the future from the commercial sector. A modularized plan, in essence planning for obsolesce in consonance with legislative direction on modularized computer hardware purchasing, will be the best

approach to maintain the balance between new technology insertion against the Agency need for procedural stability that the workforce can rely on.

1. Evidentiary Requirements

Both parties must agree to the terms and conditions of a contract or a party can raise question whether they formed a contract in the first instance. Both parties have to be certain as to what they are agreeing to in order to have the requisite intent to form a contract. If parties negotiate on the Internet without proper security, there may be doubt as to what they agreed to and what terms and conditions control since there will be no paper print out of the final agreement.

Agencies can solve this problem using available cryptography techniques that can indicate whether a document has remained unaltered and that a particular agent has signed/authenticated an electronic document. This is important to an Agency with multiple buyers and multiple buys. The Agency must develop and maintain sound business practices for establishing when an electronic contract is formed that binds the Government.

Where previously a paper document served the legal purpose of representing the agreement, now the Agency's computer operation and storage procedures will represent the agreement. The paper contract will just be a representation of what is stored in the computer. If a dispute arises and the Agency has electronic contract procedures in place, a court will not deny the agreement legal effect solely because the agreement is in an electronic form. The court can now look to how the Agency handles and secures the messages. If the Agency can prove they have a sound computer operation and storage system, they should prevail in a dispute about terms and conditions.

The rules of evidence used to prove the validity and unaltered status of an electronic contract are not overly burdensome. The Agency IT scheme must be able to satisfy those rules or an electronic contracting scheme will not work. Agency needs for what IT storage and transmission plans work will be different from Agency to Agency. For example, a distributed client/server arrangement will require a different approach than a mainframe UNIX system or any combination of client/server and mainframe currently in use.

Whatever IT solution is available or used, the Agency must be able to document the full gamut of message generation, encryption/decryption and storage in place in light of the rules of evidence before embarking on an electronic system of contracting. The Agency should seek legal counsel and IT expert advice concerning the legitimacy and sufficiency of their IT strategy for electronic contracting.

In the same vein, the idea of an original document loses meaning in an electronic contracting environment. Unlike in the paper world, where B receives a paper document from A, in an electronic environment, the contract is a copy of the message transmitted by A. Any Agency requirement for original documentation is met by an electronic message when there is a reliable assurance, usually cryptologically based, for the integrity of the information from the time when it was generated as an electronic message to delivery of the message. Maintaining the integrity of the message overlays with the ideas behind the rules of evidence for messages.

2. Attribution

An offer and acceptance may be sent by electronic messages and may form the basis of an electronic contract depending on the circumstance surrounding the attribution procedures involved. U.C.C. Article 2B envisions methods for attributing a message to a party. Proper attribution procedures are necessary as a measure of intent of the parties.

Between A and B, B is entitled to regard a data message as being from A, and to act on that assumption, if B can prove the message was sent by A by previously agreed to means and the message was really sent by A or A's agent, electronic or human. These requirements and ideas track very closely with current, applicable state laws on the matter.

An attribution rule, by operation of law, is appropriate where one party uses one of the more usual cryptology methods to assure the authenticity and reliability of a electronic message and the other party reasonably relies on such procedures, without prior agreement. The current, more usual cryptology methods are DES, RSA, PGP and variations of DES with IDEA or SKIPJACK.

An Agency must be careful how it accepts messages and attributes them back to the sending party. In order to ensure there are no decryption problems, an Agency would be wise to only accept particular encryption strategies. Since the U.C.C. rewrite is suggesting that a contract can be formed when a party receives the message and the previous paragraph suggests that a rule of law will find attribution reasonable absent some previous agreements, the best way to mitigate attribution risk is to develop an interchange agreement and a PKI agreement that specifically addresses attribution procedures and then follow those procedures and those procedures only.

3. The Laws of Agency

The concept of agency and apparent authority is retained and extended in the electronic contracting environment. An agent can be a person or a computer if both parties are aware and agree to those conditions. This is important for an agency considering expedited contracting procedures in such areas and basic ordering agreement (BOA) orders. If a computer generates a requirement and sends the requirement to the BOA holder, a contract is formed. This will decrease workload for routine orders only to the

extent that the computer generates requirements without error. Conversely, contracting officers may eventually be dealing with computer ordering agents when buying goods for the Government. A contracting officer who attempts to include Government specific clauses may find that a court, in accordance with the U.C.C. 2B rewrite, holds that the clauses were not incorporated into the agreement because the other party's computer was incapable of agreeing to the clauses.

4. Authentication

The law requires certain contracts must be in writing and signed before the contract is enforceable. For some, a document in electronic form may simply not be regarded as valid to achieve its legal purpose.[Ref. 20;p. 107] Alternatively, it may carry less weight as evidence in a court of law, or may not be capable of being used at all.[Ref. 20] These are the problems of authentication and admissibility in an electronic contracting environment.

The Digital Signature Guidelines published by the Information Security Committee Science and Technology Section of the American Bar Association defines authentication as "A process used to ascertain the identity

of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and that is has not been modified or replaced in transit [Ref. 24;p. 28]."

The traditional rationale for authenticating a document is to make sure that the document is what it purports to be in order to prove a relationship between it and an issue a litigant wants to establish. Differences in the storage and retrieval of computer printouts, as opposed to that of conventional business records, warrant a special inquiry from a court.

A court can use authentication to establish the parties identity, the acceptance of the term or contract, or to confirm the integrity of the terms as of the time of authentication. [Ref. 45;p. 74]

Authentication can be broken down into three basic schemes. First, there is user authentication. Second, there is host authentication. Third, there is message authentication, which permits documents to be digitally signed--allowing them to be traced back to the sender and preventing them from being changed in transit.[Ref. 63;p. 87]

One approach to authentication in the third instance, is FRE 901(b)(9), which provides that technological evidence can be supported by "evidence describing a process or system used to produce a result and showing that process or system produces an accurate result.[Ref. 32]"

In "*The Law of Electronic Commerce*", Benjamin Wright cites the Advisory Committee Note to FRE 901(b)(9) for the purpose of this rule:

> [T]his rule is designed especially for computer business records. Thus, competent testimony identifying, describing the function of, and confirming the accuracy of a computer system that produced a message or record is sufficient to authenticate the message or record. It is not necessary to bring the computer system itself into the courtroom for a demonstration.[Ref. 64]

In the discussion of the hearsay rule and business records exception, an evidentiary foundation is required before a court will admit computerized records under the business records exception. However, FRE 901 sets forth other, slightly looser, methods of assuring that a piece of evidence is authentic. This aids the Agency that wants to move to electronic contracting, but only if they are able to attest competently to the functions and accuracy of the computer system that produced their contract.

For authentication to work at a Federal Agency, several internal activities will have to be coordinated. Legal counsel, the IT department, requirements generation sections and the contracting department will need to interweave their efforts and develop business practices that a court will find reasonable.

Electronic messages that form the basis of the requirement will have to have adequate security. Those messages will have to be securely stored with any access duly noted or logged. There will have to be an electronic trail that shows how a requirement was formed, negotiated, agreed to and eventually contracted for.

B. SECURITY

Technology and cryptology can provide immediate verification of receipt, and verify that no defect in receipt has occurred. Two of the most widely known hash algorithms are the MD5 message digest algorithm RSA and the Secure Hash Algorithm (SHA) developed by NIST and NSA. Assuming no one discovers a flaw to either algorithm, it is unfeasible to take a hash value produced by SHA or a message digest produced by MD5 and work backward to find the input data. If A sends a file and the file generates an

MD5 or SHA fingerprint, and B runs the same hash algorithm on the file and gets the same result, the file is intact and unchanged.

This is the basis of attribution and authentication in the electronic environment. An Agency should have little or no problem with the validity of an electronic contract provided the Agency has planned for the proper cryptological security.

1. Digital Signatures

Under the U.C.C. and the GAO, a signature includes any symbol executed or adopted by a party with intention to authenticate a writing. Draft U.C.C. Article 2B uses the term "authenticate" instead of "signature", but the effect of what a signature means or does is only broadened.

Many states have already passed or are considering some form of digital signature legislation. Likewise, most of the new major online electronic commerce initiatives are based on digital signatures.

Digital signatures provide reliable authentication and document integrity that can exceed the reliability provided by traditional paper-based methods. Current legislation at the state and commercial level is staking out the positions

that identify when, and under what circumstances, the law will recognize such enhanced reliability. These are some of the areas that an Agency will need to maintain a high degree of mark

2. CA Risk

An assumption surrounding PKI is that third party CAs would handle the intermediary function of identifying parties to a contract. The CA would certify identities to allow participants to conduct business without ever meeting. There is a large, uncertain liability exposure that could prevent the emergence of commercial CAs.

There simply is a limit to what X.509 and the CA paradigm can offer regarding certificate reliance and certificate content reliance.

The CA could take every reasonable step to confirm identity, but still issue an erroneous certificate. A criminal could impose losses on a large number of third parties who would rely on an erroneous certificate. If every party who relied on the certificate had a claim against the CA for losses, the CA's potential liability could be enormous.

Without legislative relief, CAs would be forced to go to extraordinary lengths to confirm identity, at a high cost, even when the participants may have accepted a less thorough and less expensive certificate.

One last issue is that CAs have little or no control over the care a subscriber takes in protecting their private key. If CAs bear liability to third parties for stolen certificates, it will be reflected in the price of certificates, which might then be uneconomically high.

CAs face exposure if their private key is compromised. Once the compromise is discovered, all certificates issued by that CA would have to be revoked and new certificates issued, imposing costs on all of the subscribers of that CA. If CAs face liability for these potentially immense losses, entrepreneurs might choose not to enter the CA business at all.

Additionally, there is the issue of maintaining the CSL. If a subscriber checks a signature against an out-of-date or incorrect CSL, there is potential liability for the CA absent some legislative relief or definition of a minimum acceptable level of how a CSL can be maintained in a commercially reasonable fashion.

The ABA Committee released its "*Digital Signature Guidelines*" which set out duties for CAs, subscribers, and relying parties. Many states are using similar concepts that attempt to quantify and qualify where risk begins and ends for the CA, the subscriber and third party participants. The legal decisions that have affected VAN liability may spill over into this forum when the first CA case is decided. The issue is far from decided and agencies must exercise care in deciding how to frame a CA arrangement. They must also consider the liability question if they choose to be their own CA and issue certificates internally.

3. X.509

The purpose of a CA is to bind a public key to the name contained in the certificate and assure third parties that this binding is valid for both the name and key. To that end, X. 509 has been generally adopted as a mechanism for binding identities to keys.

The issue of exactly how completely linked the name and key is, is outside the scope of X.509 and depends on each CA's self-defined Certification Practice Statement (CSP).

X.509 is based on X.500, a naming scheme, but X.500 is not completely defined. X.500 was designed to be a global database of everything connected to computers. An analogy can be made of a telephone book with a listing for every connected computer terminal. To handle a database of that size, the architecture developed as a distributed database, maintained by multiple people, held in multiple locations.

To specify who had authority to change which portion of this distributed database; the X.509 certificate was designed, linking a public signature key to the distributed database.

X.509 has evolved from a mechanism for proving permission to modify a node in the X.500 data structure to an identity certificate. This is where an Agency must use caution and common sense when implementing their electronic commerce. X. 509 is the standard identification mechanism, however it is not complete and has some drawbacks.

X.509 depends on many other standards such as ISO, ANSI, ITU, and IETF and all those standards must be read in total to really understand what X.509 does. This has left room for many different interpretations of X.509.

Because there is room for interpretation, companies have implemented the standard in different ways. Both

Netscape and Microsoft use X.509 certificates, but an X.509 Certificate generated by Netscape may not be readable by Microsoft products, and vice versa. DISA's purchase of Netscape for Agency use may have solved the problem for a Federal Agency about which system to choose for themselves, but agencies will have to conduct business with the commercial sector, and the interplay of certificates may become a problem then.

X.509 allows CA's practices and policies to be predicated upon self-regulation on the issues of trust and trust management. X.509 certificate is essentially a business practice whose meaning and validity strongly depends on the individual CA. Moreover, participants may trust the confirmation procedures of the CA during certificate reliance, but they cannot rely upon certificates for other than their value as a representation of the CA's authentication management act expressed in the CA's own terms and rules in the CSP.

C. FEDERAL REQUIREMENTS

Recent legislation proposed at the Federal level adopts the Utah/ABA Guidelines model with an added twist: key escrow. Under these proposed laws, CAs not only serve

to bind subscribers to their public encryption keys used for authentication purposes, but also serve as key escrow agents, verifying the escrowing of keys used for confidentiality purposes. Key escrow is a method for the Government, notably NSA, to keep for themselves or a third party, what amounts to an encryption skeleton key that could be used to unlock encrypted message traffic. NSA claims necessity for escrowed keys in case of terrorism or other threats to national security. They want to keep the ability to decrypt messages that identify illegal activities much like a wiretap on a phone. Many groups attempting to do business on the Internet have ridiculed the idea and vilified NSA and NSA encryption products in the process. Cryptographers have alleged that DSS and DSA are faulty. Most of industry had tried to get the RSA algorithm to be the standard for digital signatures. NSA preferred DSA because, unlike RSA, DSA does not have encryption capabilities. This demonstrates NSA's great sensitivity to cryptography having an encryption function.

The dispute highlights a critical concern commercial activities have with Government, particularly NSA, involvement on the Internet. For commercial activity to be successful, the messages that contain important proprietary

data or pricing must remain secret. For NSA, secrets pose a risk to national stability. The legislative pendulum has swung back and forth on the issue.

For example, President Reagan issued the National Security Decision Directive (NSDD) 145 in 1984. The Reagan directive gave NSA control over all Government computer systems containing "sensitive but unclassified" information. This was followed by a second directive that extended NSA authority over non-Government computer systems.

In 1987, Congress enacted a law reaffirming that NIST was responsible for the security of unclassified, non-military Government computer systems. Under the 1987 law, the role of NSA was limited to providing technical assistance in the civilian security realm. Congress felt that it was inappropriate for a military intelligence Agency to have control over the dissemination of unclassified information.

In 1989, NSA signed a Memorandum of Understanding (MOU) which purported to transfer back to NSA the authority given to NIST. The MOU created a NIST/NSA technical working group that developed the controversial Clipper Chip and Digital Signature Standard. Both of these standards were

attacked because they were either not very strong or allowed NSA a trapdoor to be able to decipher encrypted material.

The NSA has worked to weaken the mandate of the Computer Security Act. In 1994, President Clinton issued Presidential Decision Directive (PDD) 29. This directive created the Security Policy Board, which has recommended that all computer security functions for the Government be merged under NSA control.

NSA is less concerned about cryptography being unbreakable for commercial use because they feel that this will allow illegal activity to go on without the Government being able to intervene. To be useful commercially on the Internet, though, secure document need to have strong encryption to prevent competitors from gaining access to the information. NIST is caught in the middle. They are proponents for the commercial applications, but they also must be face the political reality that NSA has a very strong voice in encryption policy.

The NSA is the prime driver to maintaining weakened encryption standards. Their position is understandable. As the military representative to encryption policy, they need only look back to WW II to see just how important

cryptology was to the successful execution of a war. Their position is that they need access and control in order to keep illegal acts from being hidden behind secure cryptology.

NSA efforts to control cryptology may be too late. The encryption cat is out of the bag. There is no reason to believe that non-US sources will abide by any sort of weakened standards that are set in the U.S. Their recalcitrance serves only to put U.S. companies at a disadvantage worldwide. GAO, the Government's watchdog Agency, told Congress,

> The intelligence community appears to be insisting upon the development of a different standard for U.S. industry for electronic communications between it and the Government. This separate standard is weaker than what is commercially available, is an added burden on commercial activities and raises the question whether any practical purpose would be served by the requirement. [Ref. 42;p. 1]

There is little or no chance that NSA will recuse themselves from making policy either directly or through joint activities that NIST and NSA share. NIST will not have a free hand in developing commercial standards as long as they are entangled with NSA. An Agency developing an electronic contract will have to operate in the fine line between commercial applications that extend security and

military oversight that reigns in applications. An Agency seeking to implement a commercially acceptable, not Federally sanctioned electronic contracting scheme may find an ally in NIST, but will most certainly find NSA unmoved if the contracting scheme involves commercially strong security.

D. INTERSTATE COMMERCE

The essential nature of electronic commerce challenges the notion of state boundaries as division points for different commercial rule systems.

At the Agency level, questions remain about how electronic contracting will affect jurisdictional issues in the event of a dispute. Because the Internet is so wide ranging, most users will not be aware of the distributive possibilities of their actions or necessarily intend a contact or presence in a particular location, which normally determines the forum jurisdiction. Defining where acts and people exist for such purposes becomes harder and makes increasingly less sense in cyberspace. To reduce risk, an Agency should consider establishing a choice of forum clause in an interchange agreement that establishes

which forum will hear any dispute that arises from the contract.

When it comes to the information technology sector of the economy, Utah is not the average state. Although the concentrations of the information technology industry are, predictably, in the states of Washington, California, Utah is a close third. According to the Utah Information Technologies Association, Utah currently ranks second in the world as the largest computer software development center. A Wirthlin Group survey determined that Utah has several thousand information technology related businesses in various developmental stages.[Ref. 57]

The State of Utah developed the first digital signature legislation. Under the Act, a Government Agency assumes the obligations of being a CA and, as such, is charged with policymaking, facilitating implementation of digital signature technology, and providing regulatory oversight of private sector CAs.

Licensing under the Utah Act is voluntary; however, licensed CAs are offered certain legal benefits, primarily limited liability. The Act imposes detailed duties on CAs, subscribers, and relying parties that are consistent with ABA Guidelines. In addition, it allocates liability among

these parties and gives special legal status to digitally signed documents created using the services of a licensed CA.

Being the first legislation out of the blocks, a number of states turned to the Act as model digital signature legislation, a process encouraged by the drafters of the Utah law. After enactment of the Act, digital signature legislation based on the Utah law was proposed in several states. The Act proved influential even when not expressly followed. For example, California considered and then rejected the Utah model, enacting a non-technology-specific bill designed to address transactions with Government entities.

Not all legislative bodies use the Utah/ABA Guidelines. Several states enacted legislation that addressed "electronic signatures" and other non-public key methods of authenticating electronic transmissions.

The implication for an Agency is that they must confirm in the interchange agreement and the PKI agreement which model will be used for signing a message in electronic contracting environment between the parties. Although the Utah approach is predominate now, there are

many different approaches to digital signatures available today and in the future.

Since an Agency can do business across all 50 states, the Agency must establish the legal environment that they are operating in and which rules apply. An Agency can agree to abide by the digital signature scheme in place in the state of the other party or they can attempt to negotiate a blanket digital signature arrangement with all parties in all states. If the Agency develops a single policy for digital signature usage and incorporates the policy in their interchange and PKI agreements, the problems with key management and digital signature will be greatly simplified.

E. CONCLUSION

The challenge for contract law lies in accommodating the decline in the medium of paper as a means of reflecting and concluding contractual agreements. The traditional paper document has performed many functions as evidence of agreement, as an authenticated document signed by the parties, as a means of fixing the time of agreement and the point at which the liability of the parties arose. The need has not changed, only the methodology.

If electronic commerce is not going to be limited to highly structured transactions between well-known and trusted parties, other solutions must be developed to create an effective legal framework and electronic infrastructure.

This is not the first time that technology has pushed at the legal boundaries. As hand written contracts moved on to the typewriter, there were calls that the authenticity of the document was in question because the document no longer reflected the drafters script in long hand. Instead, a mechanical device, with all the requisite opportunity for forgery, was being substituted for a time-tested method of hand-written document preparation. Telegrams, telexes, and faxes, all introduced faster and more efficient alternatives to traditional methods. All were eventually adapted and adopted into the legal mainstream as the benefits to commercial activity were realized.

Contracting on the Internet, however, challenges such time-honored paper-based doctrines as contract formation, authenticity, verifiability and admissibility.

Each of the previous technologies resulted in a paper document, and, as such, did not require any reconsideration of what a legally effective document looks like. Where

electronic contracting on the Internet is going, there is no paper.

The new computer technologies are not just more efficient means of communicating paper. Instead, these new technologies permit the negotiation, agreement, distribution and storage of documentation without ever resorting to paper. This represents the first real challenge to the underlying infrastructure of traditional commerce. requiring the legal community to implement appropriate new standards for legally effective electronics documents.

As the previous chapters have illustrated, there are numerous levels for discussion and multiple authorities with a myriad of opinion on just how electronic contracting on the Internet can work. The debates are only just beginning, and there will be numerous drafts and revisions of thought until, after several years, there is a confluence of reasoned legislative opinion, commercial activity and judicial interpretation into a substantive body of knowledge for contracting on the Internet.

Until that time, Federal agencies attempting electronic contract on the Internet will be breaking new ground with each contractual agreement.

One avenue an Agency can use to reduce exposure to risk is to develop interchange agreements and PKI agreements spelling out liabilities and responsibilities before hand. After agreements are signed, both parties would be responsible for ensuring that their agreements are updated to reflect current technology and legal thinking.

VIII. CONCLUSIONS AND RECOMMENDATIONS

A. SUMMARY AND CONCLUSIONS

1. What contract formation and authentication requirements are there to using the Internet for Government contracting?

The underlying contract formation issues have not changed by executing a contract electronically. The principal difference between a paper and an electronic contract is the method of transmission. The electronic contract has unique requirements during transmission to ensure that no changes occur. There are little or no hurdles to using the Internet for Government contracting. An Agency must expend effort maintaining adequate electronic records to meet evidence guidelines for storage, audit trail and maintenance. The rules of evidence already cover electronic records.

The technologies are in place both commercially, and, with the DISA purchase of NETSCAPE, at the Federal level to preclude interception or modification of any material while it is routing through the many nodes of the Internet. Numerous state legislatures are forming a framework to incorporate legal, electronic signatures. All standards

being developed share a common basis to determine admissibility:

- it is unique to the person using it
- it is capable of verification
- it is under the sole control of the person using it
- it is linked to data in such a manner that if the data are changed, the digital signature is invalidated
- it meets some measure of state or commercial oversight authority.

Adequate security measures are available to ensure that parties are who they say they are for authentication purposes.

2. What are some of the areas of contract formation and rules of evidence that need to be addressed before implementing a system of contracting on the Internet?

One area of evidence that needs to be addressed is how a document is securely transmitted across the open architecture of the Internet. Current cryptology answers that question irrefutably with the newest breed of encryption algorithms. PKI, with the implementing convention of a public/private key, allows users to transmit secure documents. A hash function secures identities to electronic records.

3. What security measures exist that could aid security in electronic contract formation on the Internet?

RSA is fast becoming the commercial choice for companies using the Internet for secure transactions. The Government encryption standards are often suspect since there is always the Government concern for national security. There are several other methods available to secure information on the Internet and each satisfies the requirement of being able to transmit information so that only the intended party can decrypt the message.

4. What Federal Government agencies are involved with electronic contracting on the Internet and what guidelines are already in place?

NIST and NSA are the primary agencies involved with setting cryptology standards and standards for commerce on the Internet. Several agencies, such as OMB and GAO, also have a measure of oversight in the process. The concern at the Federal level depends on the organization. NIST, as a department in the Commerce Department, is concerned with commercial application of electronic contracting and the underlying cryptology. NSA, as a department in the DOD, is concerned with security and how potential foes might use

cryptology against the United States in a military fashion or as cover for illegal activities.

The principal standards at the Federal level are the FIPS put in place by NIST. There are numerous commercial activities beside NIST that set standards. In that case, NIST is charged with interpreting and implementing those external standards into FIPS guidance.

5. What is the commercial sector and state legislatures doing about electronic contract formation?

The states, with Utah in the lead, are quickly addressing and embracing the idea of electronic contracting as a means to speed up commerce. More than 30 state legislatures are implementing or discussing enabling legislation. The NCCUSL has been rewriting the U.C.C. to account for the sea change of events that the Internet has spawned. For the most part, contract formation issues are left alone. Only issues that directly affect transmission, attribution and authentication of messages is being addressed.

6. How can Federal agencies mitigate risk while implementing electronic contracting?

A wants to send B a contract electronically and B needs an electronic signature to verify authenticity. First

A sends the document. Then he uses a hash algorithm to generate a fingerprint for the document, encrypts the hash value with his private key, and sends the encrypted hash value to B. This is A's digital signature. B uses the same hash algorithm to fingerprint the document he received and then unencrypts the hash value he received from A using A's public key. If the two hash values match, then B not only knows that the document he received is authentic, but he also knows that A's signature is real. And if the information that A sent to B is sensitive, then it can be encrypted so that only B can read it.

This model--or one similar to it--is probably the one that most participants use to conduct business. It is the basis for the U.S. Government's DSS, and the public-key cryptosystem DSA.

In order to reduce risk, agencies can agree to interchange agreements and PKI agreements to assign risk and responsibility for electronic contracting on the Internet. By documenting the process and assigning responsibility, both parties will have a clearer understanding when a contract has formed and what each party must do in order to discharge their contractual responsibilities.

a) Interchange Agreements

The concerns of any users of an electronic trading arrangement will be to ensure that the messages transmitted are genuine, that there has been no subsequent modification after transmission, that the contents of the messages have not been disclosed to third parties, that the messages are not accidentally repeated, that they are not lost within the system, that there is no unanticipated delay in the recipient receiving an uncorrupted message and that any legal relationship which the messages themselves attempt to establish is enforceable.

An Interchange Agreement allows participants to set out identification controls and methods of verifying, authenticating and attributing messages. It provides a framework for dealing with other issues such as at what stage in the transmission procedure the message is legally received by the recipient or who or what agent has what level of what kind of authority.

An Interchange Agreement can stipulate that in case of disputes, no party is entitled to raise a question of the validity of an EDI contract because they exchanged the material electronically.

An Interchange Agreement can provide that the parties each agree that computer generated records will be admissible in court if both parties maintain an agreed level of security and administrative control over their computer systems.

An Interchange Agreement allows participants the opportunity to address the contractual trading arrangements that they can establish pursuant to the messages transmitted.

Anticipating that some messages will be delivered in a garbled or unreadable fashion, a Interchange Agreement can contain a provision that imposes an obligation to provide verification of receipt. Effective verification practices as a normal course of business routine increases the opportunity for the early detection and resolution of transmission errors. This reduces the possibility of misunderstanding or lack of performance issues.

An Interchange Agreement affords the opportunity for the parties to agree which of them carries risk for error in the transmission of data, a corruption of the data on its passage through the network or the risk of the network crashing after transmission.

The American Bar Association has a Model Agreement that is both thorough and reflective of the commercial marketplace. In keeping with the original intent of the thesis, anytime a commercial alternative is available, agencies should use the alternative rather than developing their own standards unless it makes no financial or security sense.

b) PKI and CAs

PKI relies heavily on third party CA to ensure that participant identity and public keys are linked correctly. A Certificate Policy for CAs (Appendix) is necessary in establishing certificate policies suitable for electronic transactions. The Model Certificate Policy covers both Government and private CAs. The Model Certificate Policy assumes that the CA is using its own self-signed root key.

By establishing a certificate policy, an Agency can specify its requirements for the level of assurance necessary for certificates that they will use.

Certificate policies can also constitute a basis for approval of CAs. Approval may be determined through compliance with a particular certificate policy. A

certificate policy can be used to promote interoperability between CAs operated by different organizations and to facilitate the automated acceptance of certificates by relying parties.

This helps to prevent a relying party from using a certificate for a purpose other than that intended. This also prevents a signer from repudiating a signature on the basis they did not intend the signature to be used for that purpose.

From the CAs perspective, the ability to issue certificates that assert compliance with a particular certificate policy may have benefits as the CA tries to build a business base.

Being obligated to the terms of a certificate policy may expose the CA to additional liability. Issues of CA liability are discussed in chapter VII.

For relying parties, the Model Policy allows some parties to rely on the legal benefits of the certificate policy. However, the exact parameters of that classification are open and subject to further discussion.

It seems doubtful that a certificate policy can specify the rights and obligations of subscribers unless there is a contract by which the parties so agree. The

Model Policy requires the CA to sign an enforceable contract with the subscriber to define each others rights and obligations.

The Model Certificate Policy is technologically neutral so that many certification authorities operating under a variety of different CPSs can adopt it. The current draft of the Model Certificate Policy does not cover cross certification of other CAs. Certificates issued under the Model Policy are suitable for applications requiring a medium level of assurance.

B. RECOMMENDATIONS

It is recommended that Federal Agencies use the Internet to transact electronic contracts. Agencies must prepare and document their computer systems in order to meet the current laws of evidence and they must secure the messages cryptologically. Agencies should implement interchange agreements and PKI agreements the pre approve business operating procedures in order to minimize risk and misunderstanding in the electronic environment.

C. AREAS FOR FURTHER RESEARCH

There are a number of areas of research that would benefit Agencies looking to implement electronic

contracting on the Internet. The areas are Federal rules of evidence, cryptology and FIPS, and state and commercial activity and a business case analysis for electronic contracting.

1. Federal Rules of Evidence

There is any number of Federal rules of evidence that would control the issues of electronic contracting in a court of law. A thorough review of the rules and their application in the electronic environment would reduce the risk for an Agency looking to implement electronic contracting on the Internet.

2. Cryptology and FIPS

Any number of cryptological approaches could be used to secure messages across the open architecture of the Internet. Federal Agencies are limited to the use of approved FIPS procedures. A case can be made that FIPS are not always the best standards and that the Agency responsible for developing FIPS may be limited in what they can provide to other Agencies. Agencies would benefit from a disinterest third party review of the FIPS standards versus commercial products available in the marketplace.

3. State and Commercial Activity

State legislatures and the U.C.C. are both hard at work implementing policy and procedures for conducting business on the Internet. These policies and procedures will have an enormous impact on the Federal process. An Agency would be well served being kept up-to-date with a survey of the latest developments.

4. Business Case Analysis

There is any number of costs associated with implementing an electronic contracting system on the Internet. There are many Agencies with many different computing systems and many different needs for contracting capability. An Agency would be well served with a thorough business case analysis of the costs involved with implementing electronic contracting on the Internet to allow the Agency to properly staff and resource the endeavor.

APPENDIX

Government Information Technology Services
Federal PKI Task Force
Business and Legal Work Group
MODEL CERTIFICATE POLICY

1. INTRODUCTION
   - 1.1 Overview
   - 1.2 Policy Identification
   - 1.3 Community & Applicability
     - 1.3.1 Certification Authorities (CAs)
       - 1.3.1.1 CAs Authorized to Issue Certificates Under This Policy
     - 1.3.2 Registration Authorities and Certificate Manufacturing Authorities
     - 1.3.3 Repositories
     - 1.3.4 Subscribers
     - 1.3.5 Relying Parties
     - 1.3.6 Applicability
       - 1.3.6.1 Suitable Applications
   - 1.4 Contact Details

2. GENERAL PROVISIONS
   - 2.1 Obligations
     - 2.1.1 CA Obligations
       - 2.1.1.1 Representations by CA
     - 2.1.2 RA And CMA Obligations
     - 2.1.3 Repository Obligations
     - 2.1.4 Subscriber Obligations
     - 2.1.5 Relving Party Obligations
   - 2.2 Liability
   - 2.3 Financial Responsibility
   - 2.4 Interpretation & Enforcement
     - 2.4.1 Governing law
     - 2.4.2 Dispute Resolution Procedures
   - 2.5 Fees
   - 2.6 Publication & Repositories
     - 2.6.1 Publication of CA Information
     - 2.6.2 Frequency of Publication
     - 2.6.3 Access Controls
   - 2.7 Compliance Audit
   - 2.8 Confidentiality Policy

3. IDENTIFICATION AND AUTHENTICATION
   - 3.1 Initial Registration
     - 3.1.1 Types of Names
     - 3.1.2 Name Meanings
     - 3.1.3 Rules For Interpreting Various Name Forms
     - 3.1.4 Name Uniqueness
     - 3.1.5 Verification of Key Pair
     - 3.1.6 Authentication of Organizations

MODEL CERTIFICATE POLICY

1. INTRODUCTION

1.1 Overview

This Certificate Policy ("Policy") specifies minimum requirements for the issuance and management of certificates that may be used in verifying digital signatures on the categories of electronic communications specified as suitable applications in Section 1.3.6 of this Policy.

1.2 Policy Identification

This Policy [is registered with _____, and] has been assigned an object identifier (OID) of _____.

1.3 Community & Applicability

1.3.1 Certification Authorities (CAs)

This Policy is binding on each Authorized CA that issues certificates that identify this Policy, and governs its performance with respect to all certificates it issues that reference this Policy.

Specific practices and procedures by which the CA implements the requirements of this Policy shall be set forth by the CA in a certification practice statement ("CPS") or other publicly available document, or by contract [with all Qualified Relying Parties].

1.3.1.1 CAs Authorized to Issue Certificates under this Policy

[Alternate 1] Any CA may issue certificates that identify this Policy provided that such CA agrees to be bound by, and complies with, the undertakings and representations of this Policy with respect to such certificates. Issuance of a certificate that references this Policy shall constitute agreement by the issuing CA to be bound by the terms of this Policy for all certificates that reference this Policy.

[Alternate 2] A CA may issue certificates that identify this Policy only if such CA first qualifies as an Authorized CA by:

(a) entering into an agreement with [the Policy Administering Organization], for the benefit of all Qualified Relying Parties, to be bound by, and comply with, the undertakings and representations of this Policy, with respect to the class of certificates that are issued with reference to this Policy, and

(b) being approved by [the Policy Administering Organization], following successful completion of the compliance audit specified in Section 2.7, a review of
its CPS, and satisfaction of [other applicable requirements].

1.3.2 Registration Authorities and Certificate Manufacturing Authorities

See Section 2.1.2.

1.3.3 Repositories

See Section 2.1.2.

1.3.4 Subscribers

A CA may issue certificates that reference this Policy to the following classes of subscribers:

individuals (unaffiliated)

individuals associated with a sponsor recognized by the CA ("affiliated individuals"), provided the sponsor is the subscriber of a valid certificate issued
by the CA in accordance with this Policy.

organizations that qualify as legal entities

Government agencies

1.3.5 Relying Parties

This Policy is intended for the benefit of the following persons who may rely on certificates issued to others that reference this Policy ("Qualified Relying Parties"):

Federal Government agencies that specify this Policy by regulation

State Government agencies that specify this Policy by regulation

Businesses that __[contractually agree to this Policy with the Policy Administering Organization/with the CA]___

Individuals that _____

1.3.6 Applicability

1.3.6.1 Suitable Applications

In determining the categories of transactions for which certificates issued under this Policy may be used, Federal agencies need to evaluate the relative sensitivity of applications for which they intend to send and receive digitally signed messages, bearing in mind the provisions of the Computer Security Act and applicable regulations relating thereto. This section should specify the categories of transactions for which certificates issued under this Policy are considered appropriate. The inclusion of such categories should be based on a qualitative risk analysis whereby agencies should determine the level of identity binding they require for their applications. See Section 3. In making such determinations, agencies should consider the need for low value v. high value certificates, whether applications are critical or non-critical, etc.

1.4 Contact Details

This Policy is administered by ("Policy Administering Organization"):

_____

_____

_____

Attn: _____

Phone number: _____

E-mail address: _____

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA Obligations

The CA is responsible for all aspects of the issuance and management of a certificate, including control over the application/enrollment process, the identification and authentication process, the actual certificate manufacturing process, publication of the certificate, suspension and revocation of the certificate, and renewal of the certificate, and for ensuring that all aspects of the CA Services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

2.1.1.1 Representations By CA

By issuing a certificate that references this Policy, the CA certifies to the subscriber, and to all Qualified Relying Parties who reasonably and in good faith rely on the information contained in the certificate during its operational period and in accordance with this Policy, has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS that:

The CA has issued, and will manage, the certificate in accordance with this Policy

The CA has complied with the requirements of this Policy and its applicable CPS when authenticating the subscriber and issuing the certificate

There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS

Information provided by the subscriber in the certificate application for inclusion in the certificate has been accurately transcribed to the certificate

The certificate meets all material requirements of this Policy and the CA's CPS

2.1.2 RA and CMA Obligations

The CA shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. However, the CA may [delegate/subcontract] performance of these obligations to an identified registration authority ("RA") and/or certificate manufacturing authority ("CMA") provided that the CA remains primarily responsible for the performance of those services by such third parties in a manner consistent with the requirements of this Policy.

2.1.3 Repository Obligations

The CA shall be responsible for providing a repository and performing all associated functions. However, the CA may [delegate/subcontract] performance of this obligation to an identified repository services provider ("RSP"), provided that the CA remains primarily responsible for performance of those services by such third party in a manner consistent with the requirements of this Policy.

2.1.4 Subscriber Obligations

In all cases, the CA shall require the subscriber to enter into an enforceable contractual commitment [for the benefit of Qualified Relying Parties] obligating the subscriber to:

generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key

acknowledge that by accepting the certificate the subscriber is warranting that all information and representations made by the subscriber that are included in the certificate are true

use the certificate exclusively for authorized and legal purposes, consistent with this Policy

instruct the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the subscribers private key

2.1.5 Relying Party Obligations

A Qualified Relying Party has a right to rely on a certificate that references this Policy only if the certificate was used and relied upon for lawful purposes and under circumstances where:

the reliance was reasonable and in good faith in light of all the circumstances know to the relying party at the time of reliance

the purpose for which the certificate was used was appropriate under this Policy

the relying party checked the status of the certificate prior to reliance, or a check of the certificate's status would have indicated that the certificate was valid

2.2 Liability

A CA is responsible to Qualified Relying Parties for direct damages suffered by such relying parties that are caused by the failure of the CA to comply with the terms of this Policy, and sustained by such relying parties as a result of reliance on a certificate in accordance with this Policy, but only to the extent that the damages result from the use of certificates for a suitable applications listed in Section 1.3.6.

[Except as expressly provided in this Policy and in its CPS, CA disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.]

[The liability of a CA under this Policy shall be limited to direct damages, and shall not exceed _____. CA shall have no liability for consequential damages].

2.3 Financial Responsibility

No stipulation.

2.4 Interpretation & Enforcement

2.4.1 Governing Law

The enforceability, construction, interpretation, and validity of this Policy shall be governed by the laws of the United States and the State of _____

2.4.2 Dispute Resolution Procedures

No stipulation

2.5 Fees

CA shall not impose any fees on the reading of this Policy or its CPS. CA may charge access fees on certificates, certificate status information, or CRLs, subject to agreement between the CA and subscriber, and in accordance with a fee schedule published by the CA in its CPS or otherwise.

2.6 Publication & Repositories

2.6.1 Publication Of CA Information

Each Authorized CA shall operate a secure on-line repository that is available to Qualified Relying Parties and that contains (1) issued certificates that reference this Policy, (2) a Certificate Revocation List ("CRL") or on-line certificate status database, (3) the CA's certificate for its signing key, (4) past and current versions of the CA's CPS, (5) a copy of this Policy, and (6) other relevant information relating to certificates that reference this Policy.

2.6.2 Frequency of Publication

All information to be published in the repository shall be published promptly after such information is available to the CA. Certificates issued by the CA that reference this Policy will be published promptly upon acceptance of such certificate by the subscriber. Information relating to the revocation of a certificate will be published in accordance with section 4.4.3.

2.6.3 Access Controls

The repository will be available to Qualified Relying Parties [and subscribers] on a substantially 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance and the CA's then current terms of access. CA shall not impose any access controls on this Policy, the CA's certificate for its signing key, and past and current versions of the CA's CPS. CA may impose access controls on certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CA and subscriber, in accordance with provisions published in its CPS or otherwise.

2.7 Compliance Audit

Before initial approval as an Authorized CA, and thereafter at least once every year, the CA (and each RA, CMA, and RSP, as applicable) shall submit to a compliance audit by an independent nationally recognized security audit firm [approved by _____] that is qualified to perform a security audit on a CA and that has significant experience in the application of PKI and cryptographic technologies. The purpose of such audit shall be to verify that the CA has in place a system to assure the quality of the CA

Services that it provides, that complies with all of the requirements of this Policy and its CPS, and that its CPS is consistent with the requirements of this Policy.

2.8 Confidentiality Policy

Information regarding subscribers that is submitted on applications for certificates will be kept confidential by CA and shall not be released without the prior consent of the subscriber, unless otherwise required by law. The foregoing shall not apply, however, to information appearing on certificates, or to information regarding subscribers that is obtained by CA from public sources. Under no circumstances shall CA (or any RA, RSP, CMA) have access to the private keys of any subscriber to whom it issues a certificate that references this Policy.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

Subject to the requirements noted below, Certificate applications may be communicated from the applicant to the CA or an RA, (and authorizations to issue certificates may be communicated from an RA to the CA), (1) electronically via E-mail or a web site, provided that all communication is secure, such as (1) by using SSL or a similar security protocol, (2) by first class U.S. mail, or (3) in person.

3.1.1 Types of Names

The subject name used for certificate applicants shall be [the X.509 Distinguished Name].

3.1.2 Name Meanings

The subject name listed in a certificate must have a reasonable association with the authenticated name of the subscriber. In the case of individuals
this should be a combination of first name and/or initials and surname. In the case of an organization the name should reflect the legal name of the organization and/or
unit.

3.1.3 Rules For Interpreting Various Name Forms

No stipulation.

3.1.4 Name Uniqueness

The subject name listed in a certificate shall be unambiguous and unique for all certificates issued by the CA. [and conform to X.500 standards for name uniqueness]. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of certificates issued by the CA.

3.1.5 Verification of Key Pair

The CA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application [in accordance with an appropriate secure protocol, such as that described in the IETF PKIX Certificate Management Protocol or through other means].

3.1.6 Authentication of Organization

When a CA receives a certificate application from an organization, it shall conduct an independent investigation in order to determine whether:

The organization exists and conducts business at the address listed in the certificate application. The certificate application was signed by a signatory who was a duly authorized reprentative of the organization named therein. The information contained in the certificate application is correct.

In conducting its review and investigation, the CA shall review official Government records and/or engage the services of a reputable third party vendor of business information to provide validation information concerning each organization applying for a certificate, including legal company name, type of entity, year of formation, names of directors and officers, address, telephone number, and good standing in the jurisdiction where the applicant is incorporated or otherwise organized.

3.1.7 Authentication of Individual -- No Affiliation

In determining the form and type of authentication required for certificates issued pursuant to this Policy, Federal agencies should evaluate the relative sensitivity of applications for which they intend to send and receive digitally signed messages. Based on such evaluation, it may be appropriate to authorize on-line identity verification (such as proposed in the ACES program), while in other cases, it may be appropriate to require applicants to personally present themselves, or to provide notarized copies of identity papers.

3.1.8 Authentication of Individual – Affiliated Certificate

3.1.8.1 Identification

The CA may establish a trustworthy procedure whereby a sponsoring organization that has been authenticated by the CA and issued a certificate may designate one or more Responsible Individuals, and authorize them to represent the sponsoring organization in connection with the issuance and revocation of certificates for affiliated individuals. The CA may rely on a designated Responsible Individual appointed by the sponsor to properly authenticate the individual applicant (provided that the CA has previously authenticated the sponsor as an organization and the Responsible Individual as an unaffiliated individual, in accordance with this Policy). In the absence of the foregoing procedure, affiliated individuals shall be authenticated in the same manner as unaffiliated individuals.

3.1.8.2 Authentication Confirmation Procedure

Authentication of the individual will be confirmed through the use of a shared secret [such as a PIN number] that is distributed via a trustworthy out of band communication to the applicant (either directly or via the sponsor) and included in the application process as part of the certificate enrollment process.

3.1.8.3 Personal Presence

Applicants that are affiliated with [an Approved] sponsor can be authenticated through an electronically submitted application, based on an appropriate agreement with the sponsor, the approval of a designated Responsible Individual, and the distribution of PIN numbers or a similar security device.

3.1.8.4 Duties of Responsible Individuals

The Responsible Individual represents the sponsoring organization with respect to the issuance and management of certificates. In that capacity he or she is responsible for properly indicating which subscribers are to receive certificates.

3.2 Renewal Applications (Routine Rekey)

Within _____ months prior to the scheduled expiration of the operational period of a certificate issued following authentication under this Policy, a subscriber may request issuance of a new certificate for a new key pair from the CA that issued the original certificate, provided the original certificate has not been suspended or revoked. Such a request may be made electronically via a digitally signed message based on the old key pair in the original certificate.

3.3 Rekey After Revocation

Revoked or expired certificates shall not be renewed. Applicants without a valid certificate from the CA that reference this Policy shall be re-authenticated by the CA or RA on certificate application, just as with a first-time application.

3.4 Revocation Request

A revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the old key pair. The identity of a person submitting a revocation request in any other manner shall be authenticated [in accordance with Section ___]. Revocation requests authenticated on the basis of the old (compromised) key pair shall always be accepted as valid. Other revocation request authentication mechanisms may be used as well. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

An applicant for a certificate shall complete a certificate application in a form prescribed by the CA and enter into a subscriber agreement with the CA. All applications are subject to review, approval and acceptance by CA. The certificate application process may be initiated by the following persons:

Potential Subscriber	Authorized Initiator
Individual (unaffiliated)	Potential subscriber only
Individual affiliated with a sponsor	Potential subscriber or duly authorized representative of sponsor

Organization	Duly authorized representative of potential subscriber only

4.2 Certificate Issuance

Upon successful completion of the subscriber identification and authentication process in accordance with this Policy, and complete and final approval of the certificate application, the CA shall issue the requested certificate, notify the applicant thereof, and make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the subscriber only. A CA will not issue a certificate without the consent of the applicant and, if applicable, the applicant's sponsor.

4.3 Certificate Acceptance

Following issuance of a certificate, the CA shall contractually require the subscriber to expressly indicate acceptance or rejection of the certificate to the CA, in accordance with procedures established by the CA and specified in the CPS.

4.4 Certificate Revocation

4.4.1 Circumstances For Revocation

4.4.1.1 Permissive Revocation

A subscriber may request revocation of his, her, or its certificate at any time for any reason. A sponsoring organization (where applicable) may request revocation of the certificate of any affiliated individual at any time for any reason. [The issuing CA may also revoke a certificate upon failure of the subscriber (or the sponsoring organization, where applicable) to meet its obligations under this Certificate Policy, the applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force.]

4.4.1.2 Required Revocation

A subscriber, or a sponsoring organization (where applicable) shall promptly request revocation of a certificate:

whenever any of the information on the certificate changes or becomes obsolete

whenever the private key, or the media holding the private key, associated with the certificate is, or is suspected of having been, compromised

whenever an affiliated individual is no longer affiliated with the sponsor

The issuing CA shall revoke a certificate:

upon request of the subscriber or sponsoring organization

[upon failure of the subscriber (or the sponsoring organization, where applicable) to meet its material obligations under this Certificate Policy, any applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force.]

if knowledge or reasonable suspicion of compromise is obtained

if the CA determines that the certificate was not properly issued in accordance with this Policy and/or any applicable CPS

In the event that the CA ceases operations, all certificates issued by the CA shall be revoked prior to the date that the CA ceases operations.

4.4.2 Who Can Request Revocation

The only persons permitted to request revocation of a certificate issued pursuant to this Policy are the subscriber, the sponsoring organization (where applicable), and the issuing CA.

4.4.3 Procedure For Revocation Request

A certificate revocation request should be promptly communicated to the issuing CA, either directly or through an RA. A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the subscriber, or the sponsoring organization (where applicable). Alternatively the subscriber, or sponsoring organization (where applicable), may request revocation by contacting the CA or an authorized RA in person and

providing adequate proof of identification in accordance with this Policy.

4.4.3.1 Repository/CRL Update

Promptly following revocation, the CRL or certificate status database in the repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the CA shall be archived.

4.4.4 Revocation Request Grace Period

Requests for revocation shall be processed within ____ (__) hours/working days of receipt by the CA.

4.4.5 Certificate Suspension

The procedures and requirements stated for certificate revocation must also be followed for certificate suspension where implemented.

4.4.6 CRL Issuance Frequency

When CRLs are used, an up-to-date CRL shall be issued at least every ____ hours.

4.4.7 On-Line Revocation/Status Checking Aavailability

Whenever an on-line certificate status database is used as an alternative to a CRL, such database shall be updated no later than ___ hours after revocation.

4.5 Computer Security Audit Procedures

All significant security events on the CA system should be automatically recorded in audit trail files. The audit log shall be processed at least once a week. Such files shall be retained for at least six (6) months onsite, and thereafter shall be securely archived as per Section 4.6.

4.6 Records Archival

4.6.1 Types Of Records Archived

The following data and files must be archived by [or on behalf of] the CA:

All computer security audit data

All certificate application data

All certificates, and all CRLs or certificate status records generated

Key histories

All correspondence between the CA and RAs, CMAs, RSPs, and/or subscribers

4.6.2 Retention Period For Archive

Archive of the key and certificate information must be retained for at least 30 years. Archives of the audit trail files must be retained for at least six (6) months.

4.6.3 Protection Of Archive

The archive media must be protected either by physical security alone, or a combination of physical security and cryptographic protection. This protection must be to at least the level required of the _____. It should also be provided adequate protection from environmental threats such as temperature, humidity and magnetism.

4.6.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

4.6.5 Archive Collection System (Internal Or External)

No stipulation.

4.6.6 Procedures To Obtain And Verify Archive Information

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives and if either copy is found to be corrupted or damaged in any way it shall be replaced with the other copy held in the separate location.

4.7 Key Changover

No stipulation.

4.8 Compromise And Disaster Recovery

4.8.1 Disaster Recovery Plan

The CA must have in place an appropriate disaster recovery/business resumption plan and must set up and render operational a facility located in a geographic diverse area that is capable of providing CA Services in accordance with this Policy within _____ hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be

[detailed/referenced] within the CPS or other appropriate documentation available to Qualified Relying Parties.

4.8.2 Key Compromise Plan

The CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by the CA to issue certificates, or used by any higher level CA. Such plan shall include procedures for revoking all affected certificates and promptly notifying all subscribers and all Qualified Relying Parties.

4.9 CA Termination

In the event that the CA ceases operation, all subscribers, sponsoring organizations, RAs, CMAs, RSPs, and Qualified Relying Parties will be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All certificates issued by the CA that reference this Policy will be revoked no later than the time of termination.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Security -- Access Controls

The CA, and all RAs, CMAs and RSPs, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 5.2.1. Access shall be controlled through the use of: electronic access controls, mechanical combination locksets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

5.2 Procedural Controls

5.2.1 Trusted Roles

All employees, contractors, and consultants of CA (collectively "personnel") that have access to or control over cryptographic operations that may materially affect the CA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA's repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA's operations.

5.2.2 Multiple Roles (Number Of Persons Required Per Task)

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a CA server should be shared by multiple roles and individuals. Each account on the CA server shall have limited capabilities commensurate with the role of the account holder.

5.3 Personal Security Controls

5.3.1 Background And Qualifications

CAs, RAs, CMAs, and RSPs shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy.

5.3.2 Background Investigation

CAs shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

5.3.3 Training Requirements

All CA, RA, CMA, and RSP personnel must receive proper training in order to perform their duties, and update briefings thereafter as necessary toremain current.

5.3.4 Documentation Supplied To Personnel

All CA, RA, CMA, and RSP personnel must comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, and revocation, and software functionality.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation And Installation

6.1.1 Key Pair Generation

Key pairs for CAs, CMAs, RAs, RSPs, and subscribers must be generated in such a way that the private key is not known by other than the authorized user of the key pair. Acceptable ways of accomplishing this include:

Having all users (CAs, CMAs, RAs, RSPs, and subscribers) generate their own keys on a trustworthy system, and not reveal the private keys to anyone else

Having keys generated in hardware tokens from which the private key cannot be extracted.

CA, RA, and CMA keys must be generated in hardware tokens. Key pairs for RSPs, and end-entities can be generated in either hardware or software.

6.1.2 Private Key Delivery To Entity

See Section 6.1.1.

6.1.3 Subscriber Public Key Delivery To CA

The subscriber's public key must be transferred to the RA or CA in a way that ensures that (1) it has not been changed during transit; (2) the sender possesses the private key that corresponds to the transferred public key; and (3) the sender of the public key is the legitimate user claimed in the certificate application.

6.1.4 CA Public Key Delivery To Users

The public key of the CA signing key pair may be delivered to subscribers in an on-line transaction in accordance with IETF PKIX Part 3, or via another appropriate mechanism.

6.1.5 Key Sizes

[Federal agencies should: (1) define the acceptable algorithms (e.g., RSA signature, DSA,etc.; and (2) specify the minimum key sizes for: CA signing key and user signing key for each algorithm.]

6.2 CA Private Key Protection

The CA (and the RA, CMA, and RSP) shall each protect its private key(s) in accordance with the provisions of this Policy.

6.2.1 Standards For Cryptographic Module

CA signing key generation, storage and signing operations shall be on a hardware cryptomodule rated at FIPS 140-1 Level 2 (or higher). Subscribers shall use FIPS 140-1 Level 1 approved cryptographic modules (or higher).

6.2.2 Private Key (N-M) Multi-Person Control

No stipulation.

6.2.3 Private Key Escrow

CA signing private keys shall not be escrowed.

6.2.4 Private Key Backup

An entity may optionally back up its own private key.

6.2.5 Private Key Archival

An entity may optionally archive its own private key.

6.2.6 Private Key Entry Into Cryptographic Module

No stipulation.

6.2.7 Method Of Activating Private Key

No stipulation.

6.2.8 Method Of Deactivating Private Key

No stipulation.

6.2.9 Method Of Destroying Private Key

Upon expiration or revocation of a certificate, or other termination of use of a private key for creating signatures, all copies of the private key shall be securely destroyed.

6.3 Other Aspects Of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Key Replacement

CA key pairs must be replaced at least every _____ years. RA and subscriber key pairs must be replaced not less than every _____ years and a new certificate issued.

6.3.3 Restrictions On CA's Private Key Use

The CA's signing key used for issuing certificates that conform to this Policy shall be used only for signing certificates and, optionally, CRLs. A private key used by an RA or RSP for purposes associated with its RA or RSP function shall not be used for any other purpose without the express permission of the CA.

A private key held by a CMA and used for purposes of manufacturing certificates for the CA is considered the CA's signing key, is held by the CMA as a fiduciary for the CA, and shall not be used for any reason without the express permission of the CA. Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the CA.

6.4 Activation Data

No stipulation.

6.5 Computer Security Controls

All CA servers must include the following functionality either provided by the operating system, or through a combination of operating system, PKI application, and physical safeguards: _____.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system design and development shall be conducted using a methodology that _____.

6.6.2 Security Management Controls

6.7 Network Security Controls

The CA server and repository must be protected through application level (proxy) firewalls (or separate ports of a single firewall) configured to allow only the protocols and commands required for the CA's services.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

Certificates that reference this Policy shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages -- i.e., public keys used for digital signature verification.

All certificates that reference this Policy will be issued in the [X.509 version 3] format and will include a reference to the OID for this Policy within the appropriate field. The CPS shall identify the certificate extensions supported, and the level of support for those extension, [consistent with the profile developed by the FPKI-TWG].

7.2 CRL Profile

If utilized, CRLs will be issued in the [X.509 version 2] format. The CPS shall identify the CRL extensions supported and the level of support for these extensions. [consistent with the profile developed by the FPKI-TWG]

8. POLICY ADMINISTRATION

8.1 Policy Change Procedures

8.1.1 List Of Items

Notice of all proposed changes to this Policy under consideration by the Policy Administering Organization that may materially impact users of this Policy (other than editorial or typographical corrections, or changes to the contact details) will be provided to Authorized CAs, and will be posted on the World Wide Web site of the Policy Administering Organization. Authorized CAs shall post notice of such proposed changes in their repositories and shall advise their subscribers, in writing or by e-mail, of such proposed changes.

8.1.2 Comment Period

Impacted users may file comments with the Policy Administering Organization within 45 days of original notice. If the proposed change is modified
as a result of such comments, a new notice of the modified proposed change shall be given.

8.2 Publication & Notification Procedures

A copy of this Certificate Policy is available in electronic form on the Internet at _____, and via e-mail from _____. Authorized CAs shall post copies of this Policy in their repositories.

9. DEFINITIONS

Affiliated Individual. An affiliated individual is the subject of a certificate that is affiliated with a sponsor approved by the CA (such as an employee affiliated with an employer). Certificates issued to affiliated individuals are intended to be associated with the sponsor and the responsibility for authentication lies with the sponsor.

Authorized CA. Means a certification authority that has been authorized by the Policy Administering Organization to issue certificates that reference this policy.

CA. Certification Authority

Certificate. A record that, at a minimum: (a) identifies the certification authority issuing it; (b) names or otherwise identifies its subscriber; (c) contains a public key that corresponds to a private key under the control of the subscriber; (d) identifies its operational period; and (e) contains a certificate serial number and is digitally signed by the certification authority issuing it. As used in this Policy, the term of "Certificate" refers to certificates that expressly reference this Policy in the "certificatePolicies" field of an X.509 v.3 certificate.

CMA. See Certificate Manufacturing Authority

Certificate Manufacturing Authority" (CMA). An entity that is responsible for the manufacturing and delivery of certificates signed by a certification authority, but is not responsible for identification and authentication of certificate subjects (i.e., a CMA is delegated or outsourced the task of actually manufacturing the certificate on behalf of a CA).

Certificate Revocation List (CRL). A time-stamped list of revoked certificates that has been digitally signed by a certification authority.

Certification Authority. A certification authority is an entity that is responsible for authorizing and causing the issuance of a certificate. A certification authority can perform the functions of a registration authority (RA) and a certificate manufacturing authority (CMA), or it can delegate or outsource either of these functions to separate entities.

A certification authority performs two essential functions. First, it is responsible for identifying and authenticating the intended subscriber to be name in a certificate, and verifying that such subscriber possesses the private key that corresponds to the public key that will be listed in the certificate. Second, the certification authority actually creates (or manufactures) and digitally signs the certificate. The certificate issued by the certification authority then represents that certification authority's statement as to the identity of the person named in the certificate and the binding of that person to a particular public-private key pair.

Certification Practice Statement (CPS). A "certification practice statement" is a statement of the practices that a certification authority employs in issuing, suspending, and revoking certificates and providing access to same.

CMA. See Certificate Manufacturing Authority.

CPS. See Certificate Practices Statement.

CRL. See Certificate Revocation List.

FIPS. Federal Information Processing Standards. These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to Agency waiver procedures.

IETF. Internet Engineering Task Force. The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Key pair. Means two mathematically related keys, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

RA. See "Registration Authority."

Object Identifier. An object identifier is a specially-formatted number that is registered with an internationally-recognized standards organization.

OID. See Object Identifier.

Operational Period Of A Certificate. The operational period of a certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate or is earlier revoked or suspended.

PIN. Personal Identification Number

PKI. Public Key Infrastructure

PKIX. An IETF Working Group developing technical specifications for a PKI components based on X.509 Version 3 certificates.

Policy. Means this Certificate Policy.

Policy Administering Organization. The entity specified in Section 1.4.

Private Key. Means the key of a key pair used to create a digital signature. This key must be kept a secret.

Public Key. Means the key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via a certificate issued by a certification authority and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

RA. See Registration Authority.

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party. A recipient of a digitally signed message who relies on a certificate to verify the digital signature on the message.

Repository. A trustworthy system for storing and retrieving certificates and other information relating to those certificates.

Repository Services Provider (RSP). An entity that maintains a repository accessible to the public [or at least to relying parties] for purposes of obtaining copies of certificates and/or verifying the status of such certificates.

Responsible Individual. A person designated by a sponsor to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke A Certificate. Means to prematurely end the operational period of a certificate from a specified time forward.

RSP. See Repository Services Provider.

Sponsor. An organization with which a subscriber is affiliated (e.g., as an employee, user of a service, business partner customer etc.).

Subject. A person whose public key is certified in a certificate. Also referred to as a "subscriber".

Subscriber. A subscriber is a person who (1) is the subject named or identified in a certificate issued to such person and (2) holds a private key that corresponds to a public key listed in that certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed. See "subject."

Suspend a certificate. Means to temporarily suspend the operational period of a certificate for a specified time period or from a specified time forward.

Trustworthy System. Means computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Valid Certificate. Means a certificate that (1) a certification authority has issued, (2) the subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a certificate is not "valid" until it is both issued by a certification authority and has been accepted by the subscriber.

LIST OF REFERENCES

1 22 C.F.R. @@ 120-130, as amended by 58 Fed. Reg. 39 (1995)

2 "A Framework for Global Electronic Commerce: An Executive Summary," Web/Online Service Information 1998

3 "A Practical Guide for Legal Counsel On Mitigation of Risk From Electronic Records," http://www.surety.com/ in_news/legalgid.html June 22, 1995

4 "Abrams, Marshall D, and Podell, Harold J., "Cryptography", Information Security: A Collection of Essays Marshall D. Abrams, Sushil Jajodia, Harold Podell.Ed.

5 "An Act Concerning Digital Signatures," http://www.ink.org /public/legislative/enrollbill/2059.html 1998

6 "An Act Relating to a Digital Signature," http://www. capitol.state.tx.us/cgi-bin/ tlo/textframe 1997

7 "An Act Relating to Records; Enacting the Electronic Authentication of Documents; Creating a Central Registry for Authenticating Electronic Documents; Making an Appropriation," http://legis.state.nm. us/scripts /bill_explorer.asp 1996

8 "An Act to Add Section 16.5 to the Government Code, Relating to Digital Signatures," http://www.gcwf.com /articles\digsig.htm February 24, 1995

9 Barassi, Theodore S.,"Electronic Signature Differs From Digital," New York Law Journal New York November 28, 1995

10 Biagi, Susan.,"How the Government Looks at Security," The Network Journal December, 1994

11 Bockanic, William N. ; Lynn, Marc P. Electronic Contracts Law and Technology," Journal of Systems Management July 1995

12 Braucher, Jean., "The U.C.C. Gets Another Rewrite: Just when You Thought You Really Knew the Uniform Commercial Code, Almost Every Article is Undergoing Changes in a Major Revision," ABA Journal October, 1996

13 Brinkley, Donald L, and Schell, Roger R., "Concepts and Terminology for Computer Security," Information Security: A Collection of Essays Marshall D. Abrams, Sushil Jajodia, Harold Podell. (Ed.)

14 Byczkowski, John., "Uncrackable Code Gives E-Mail Privacy," The Cincinnati Enquirer, November 19, 1995

15 "Circular No. A-119," http://www1.whitehouse.gov/WH/EOP/OMB/html/circulars/a119/a119.html#5 1998

16 "Commonwealth's Use of Electronic Signatures," http://leg1. state.va.us/cgi-in/legp504?981+ful+SB153ER 1998

17 "Computer Data Authentication," http://www.dice.ucl.ac.be/ crypto/standards/fips/html/fip113.htm 1998

18 "Computer Security Act of 1987 Public Law 100-235 (H.R. 145)," http://www.epic.org/crypto/csa/ January 8, 1988

19 "Computer Security Roles of NIST and NSA," http://bilbo.isu.edu/security/csl/csl02-91.html February, 1991

20 "Computers and the Law: Digitized Documents not to be Used in Evidence," Information Access September, 1993

21 Cyclic Redundancy Check (CRC)," http://bbs-koi.uniinc.msk.ru/tech1/1994/er_cont/crc.htm 1994

22 Cyclic Redundancy Checking," http://whatis.com/crc.htm 1998

23 "Defense Information Systems Agency," http://www.disa.mil/cmd/pao01.html 1998

24 Digital Signature Guideline Legal Infrastructure for Certification Authorities and Secure Electronic Commerce Information Security Committee Electronic Commerce and Information Technology Divisions Section of Science and Technology American Bar Association August 1, 1996

25 Du Rea, Mary V. ; Pemberton, J. Michael., "Electronic Mail and Electronic Data Interchange:Challenges to Records Management," Records Management Quarterly October, 1994

26 "Electronic Signature Act of 1996," http://www.leg.state fl.us/session/1996/senate/ bills/bill text /html/ billtext/sb0942.html 1998

27 "Electronic Signatures," http://leginfo.leg.wa.gov/pub /billinfo/senate/5300-5324/5308-s_sl_060397 1997

28 "Encryption Choice Favors RSA over NIST," Open Systems Communication April 20, 1994

29 Farnsworth, E. Allen., Contracts, Little, Brown & Company, Boston, 1990

30 "Federal Public Key Infrastructure Key Recovery Demonstration Project," http://gits-sec.dyniet.com/fpki.htm 1998

31 Federal Register Vol. 59, Department of Commerce (DOC) National Institute of Standards and Technology (NIST) [Docket No. 940535-4135] "Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS)" 59 FR 26208, May 19, 1994

32 Federal Rules of Evidence, 1998

33 Goodbody, A. L., "An Overview Of The Legal Implications Of Internet Trading," Business Monitor July 14, 1997

34 Hellman, Martin E., "Implications of Encryption Policy on the National Information Infrastructure," The Computer Lawyer February, 1994

35 "How to Satisfy the Law in an Electronic Purchasing Environment," IOMA Supplier Selection & Management Report April 1997

36 "Internet Community Rallies To Create PGP/MIME (RFC 2015) Standard For Private Electronic Mail," Business Wire January 27, 1997

37 Kehoe, Louise., "U.S. Internet Security Group Acquires Rival," Financial Times (London) April 16, 1996

38 "Key Management Issues for Public Key Cryptography," http://www.cs.sandia.gov/~mccurley/health/node18.html 1998

39 "Law Lags Behind Digital Signatures," Electronic Commerce News April 21, 1997

40 Massey, James L., "Contemporary Cryptology; An Introduction Contemporary," Cryptology The Science of Information Integrity Gustavus Simmons (Ed.)

41 McCormack on Evidence Cleary Ed 1984

42 Messmer, Ellen., "NIST Stumbles on Proposal for Public-Key Encryption," Network World July 27, 1992

43 "Minnesota Electronic Authentication Act." http://www.revisor.leg.state.mn.us/cgibin/bldbill.pl?bill=S0173.1&session=ls80 1998

44 National Conference of Commissioners on Uniform State Laws, 1993-94 Reference Book 1994

45 National Conference of Commissioners on Uniform State Laws. "Uniform Commercial Code Article 2B-Licenses" 1998

46 "National Institute of Standards and Technology," http://www.itl.nist.gov 1998

47 NTISSP No. 2, "National Policy on Protection of Sensitive, But Unclassified Information in Federal Government Telecommunications and Automated information Systems". 29 October 1986

48 "Overview of the NIST Public Key Infrastructure Program," http://csrc.nist.gov/pki/program /welcome.html February 20, 1998.

49 Prosise, Jeff., "Digital Signatures:How They Work," PC Magazine April 9, 1996

50 "Q & A Some Executive Advice," http://www.ncsa.com /magazine/ March, 1998

51 Rosenblum, Jerald E., "The U.C.C. Provides Comprehensive Provisions for Buyers and Sellers," Intellectual Property Today July, 1997

52 "Safety in Cyberspace," http://www.johnsontech.com /security.htm 1998

53 See recommendations of Article 2 Study Committee and August 1994 Draft Revisions of the Drafting Committee of the National Conference of Commissioners on Uniform State Laws and the American Law Institute August, 1994

54 Shanker, Morris G., "In Defense of the Sales Statute of Frauds and Parole Evidence Rule: A Fair Price of Admission to the Courts," Commercial Law Journal Fall 1995

55 Summary of Electronic Commerce and Digital Signature Legislation," http://www.mbc.com June 2, 1998

56 Tanenbaum, William A., "Computer Security and Encryption FAQ," The Computer Lawyer July, 1997

57 "Technology 2000-Utah's Electronic Highway," http;//www. governor.state.ut.us/sitc/ tech2000/back/itconcen.htm 1998

58 "The Digital Signature Standard proposed by NIST; National Institute of Standards and Technology," Communications of the ACM Association for Computing Machinery Inc. 1992

59 "The Use of Digital Certificates Issued by Certification Authorities will soon Become Routine Procedure in the World of Electronic Commerce," http://www.ncsa.com/magazine/ 1998

60 There are court cases involving special statutory "writing" requirements where an electronic record would not suffice because of particular policy requirements.

61 Ubois, Jeff., "Digital Signature Standard Approved; the National Institute of Standards and Technology's Digital Signature Standard for Unclassified Information," Midrange Systems August 12, 1994

62 "UNCITRAL, Draft Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication," Working Group, 28th Session Vienna October, 1994

63 "Who Goes There?" Data Communications November, 1997

64 Wright, Benjamin., The Law of Electronic Commerce, Little Brown and Company, Boston July, 1996

65 "X.509," http://www.zdwebopedia.com/X_509.htm 1998

66 Yukins, Christopher R., "Managing Electronic Commerce on the Federal Acquisition Computer Network (FACNET)", National Contract Management Journal, 1996

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center.....2
   8725 John J. Kingman Rd. STE 0944
   Fort Belvoir, Virginia 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Defense Logistics Studies Information Exchange.....2
   U.S. Army Logistics Management College
   Fort Lee, Virginia 23801-6043

4. Dr. David V. Lamm, Code SM/Lt.....5
   Department of Systems Management
   Naval Post Graduate School
   Monterey, California 93943-5101

5. Professor Mark Stone, Code SM/St.....1
   Department of Systems Management
   Naval Post Graduate School
   Monterey, California 93943-5101

6. Dr. William Haga, Code SM/Hg.....1
   Department of Systems Management
   Naval Post Graduate School
   Monterey, California 93943-5101

7. LCDR Joseph F. Dunn.....2
   Naval Air Systems Command
   Code 02
   21663 Mainsail Drive
   Lexington Park, Maryland 20653